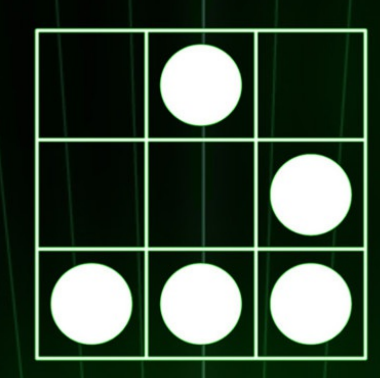
Mercè Molist Ferrer



Hackstory.es

La historia nunca contada del underground hacker en la Península Ibérica

> Enter login: #####
> Enter passw: _



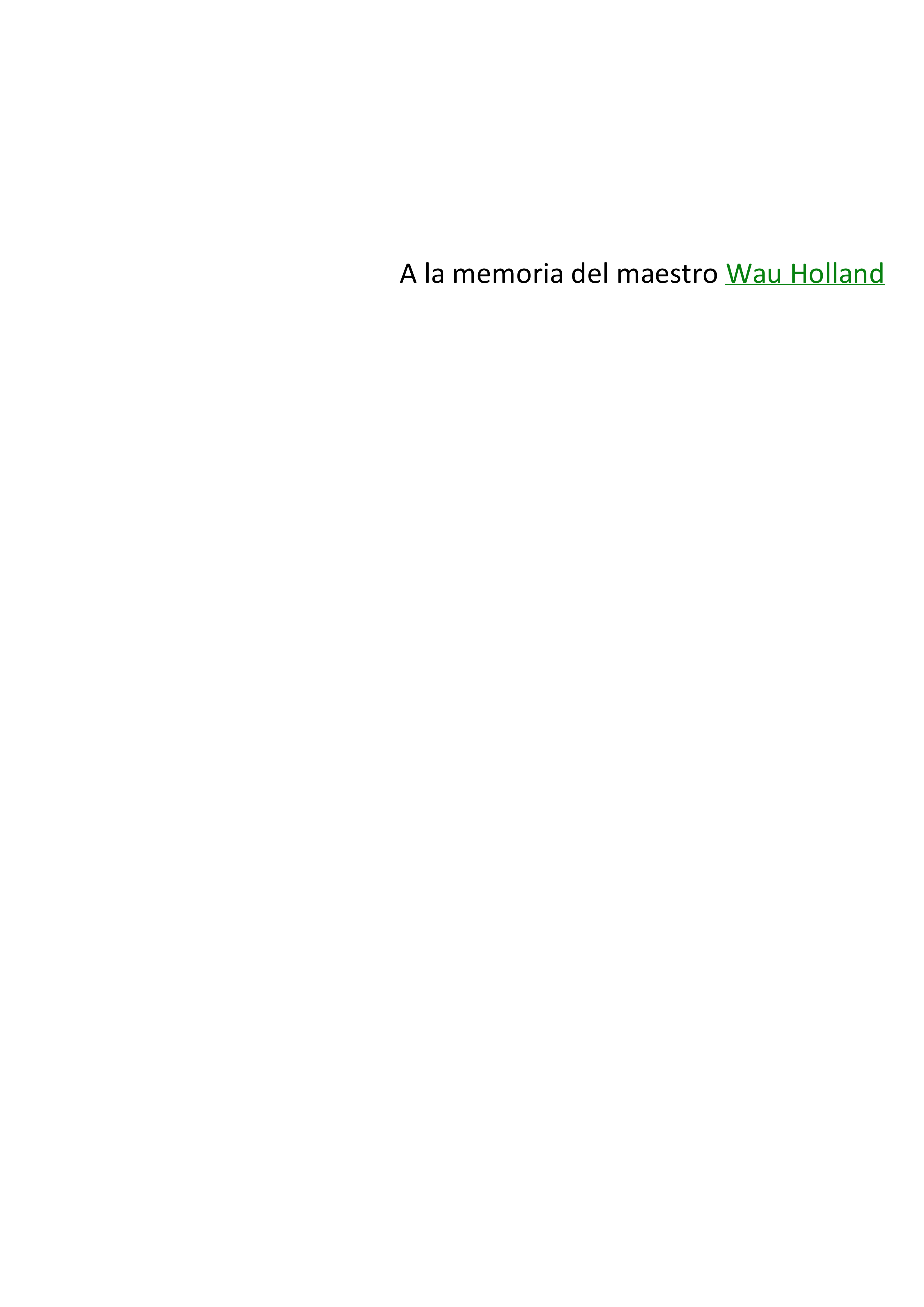




ISBN: 978-84-616-8055-9

Hackstory.es

La historia nunca contada del *underground* hacker en la Península Ibérica



A la memoria del maestro Wau Holland

Índice General

Prólogo de Zhodiac

Hay historias que no merecen ni deberían ser olvidadas. La historia del hacking español es la historia de cómo unos jóvenes, con una extrema inquietud de aprender, evolucionaron a lo que hoy en día es la defensa (y la no tan defensa) en la red de múltiples organismos nacionales e internacionales. Es la historia del aprendizaje no reglado, sin medios al alcance del bolsillo y muchas veces al margen de la ley.

Estos hackers aún viniendo de muy diferentes contextos tenían algunos puntos en común claramente diferenciados con el resto de la sociedad:

La inquietud por aprender: Cualquier cosa relacionada con la tecnología era buen candidato... arquitectura de redes, protocolos, sistemas operativos, hardware, explotación de vulnerabilidades, detección de intrusos, etc. Un abanico ingenuamente amplio que no los detenía.

La adicción adrenalínica de jugar en la red con lo aprendido: Debido a la falta de medios, todo lo aprendido se probaba sin miedo en la red contra normalmente servidores de universidades, gobiernos y a veces individuos. Nunca con un objetivo destructivo o monetario... siempre con un objetivo educacional.

El afán de colaborar: No hay que negar u ocultar el afán de reconocimiento... existía. Todo lo aprendido, evolucionado y probado se ponía a disposición pública para la continua evolución de la comunidad hacker.

Como dirían los americanos "fast forward today" muchas de estas características lamentablemente se han perdido. La entrada del dinero en este sector aniquiló este sentimiento o forma de vida hacker. Nuevos acomodados consultores con aires de prepotencia sin ganas de evolucionar, recursos al alcance de bolsillos modestos y, lo más importante, la falta de colaboración. La información es dinero y el dinero genera avaricia.

Una vez este estilo de vida fue perdido, es importante documentarlo para que, en un futuro, pueda ser revivido en esta u otra faceta. Me preguntaba la autora quién querrá leer este libro, fácil respuesta, nuestra descendencia. Estoy seguro que nuevos y románticos hackers en múltiples disciplinas revivirán este sentimiento y aprenderán que un hobby no debe ser viciado por el dinero. Llegado tal momento, lamentablemente deja de ser un hobby.

Fermin J. Serna aka Zhodiac <zhodiac@hispahack.com>

Prólogo de MegadetH

Hackers, ese término que muchos asocian con fisgones o ladrones de datos o con personajes creadores de malware, no pudiendo estar más equivocados, porque ¿qué es un hacker?, podemos decir que es aquel que conoce y disfruta con algo, y quiere aprender más y sacarle más rendimiento o partido a ese algo, en definitiva eso es lo que todos hemos querido siempre, aprender y disfrutar de ello, el sentimiento que te invade cuando estás probando un "exploit" que acabas de programar (quizás en los últimos tres días en los que nadie te ha visto el pelo), cuando estás haciendo pruebas sobre una máquina o una red, o cuando puedes comprender y mejorar el funcionamiento de un sistema operativo o un procesador, es indescriptible, y se convierte en un motivo para seguir adelante.

Para los externos a este mundo, e incluso al mundo de la informática, basta decir que el PC, el desarrollo de Internet o el sistema operativo Linux, por ejemplo, son obra de hackers.

En este caso, como seguramente habéis adivinado ya, vamos a hablar de y con hackers informáticos, qué son los hackers por excelencia, y sobre todo de sus conocimientos en el campo de la seguridad informática, ese campo tan importante al que todos hemos contribuido y que era prácticamente inexistente cuando se empezó a crear y dar servicios y conexiones sobre Internet, en definitiva esta obra recoge la historia de gente que motivada por los conocimientos y los retos tecnológicos, y a veces siguiendo una ética propia, conocemos incluso mejor que las propias multinacionales y los gobiernos, las redes de comunicaciones, los sistemas y el software, pilares básicos en la sociedad de las comunicaciones de hoy.

Seguramente todos conocemos grandes hackers, y quizás la historia de muchos de ellos, pero ¿qué conocemos realmente de la historia de los hackers y grupos de nuestro país o de habla hispana? Realmente en nuestro país ha habido y hay, desde hace mucho tiempo, hackers de gran nivel, multitud de grupos, documentación, revistas electrónicas y todo un mundo "underground" que tuvo una gran explosión en los años 90, unida a la expansión de Internet.

En esta obra, que Mercè, conocedora del mundillo como nadie, ha estado elaborando con un gran trabajo de investigación, fruto en gran parte por su pertenencia desde siempre a ese mundillo hacker, se tiene el tesoro de una parte de la historia, la historia de los hackers hispanos.

José M Mejía (MegadetH a.k.a TheGreatMega)

Prólogo de Altair Div

Muchas veces leo "noticias" relacionadas con los "hackers" en la prensa, nótese las comillas.

La gran mayoría de esas veces, dichas "noticias" relatan que alguien ha entrado en algún sistema, generalmente de forma ilegal, y hecho algún destrozo o robado datos.

Dado que en este prólogo voy a exponer mi punto de vista, me voy a permitir poner en duda que lo que reflejan esas "noticias" se corresponda con la realidad, ni tan siquiera con los llamados "hackers". En mi opinión dichas "noticias" buscan, ante todo, notoriedad muchas veces con datos deliberadamente inexactos o incompletos. Al fin y al cabo el objetivo de la publicación es vender. Los ingresos mandan y los ingresos se obtienen vendiendo. Así son las cosas.

Deberíamos conocer primero dos cosas: qué es un hacker, y luego la diferencia entre el "hacker bueno" y el "hacker malo".

De forma general un hacker es alguien con un nivel de conocimientos en un área superior al de la mayoría. El término "hacker" se suele aplicar al género de la informática, pero lo cierto es que se puede aplicar a cualquier profesión.

Wolfgang Amadeus Mozart fue un hacker de la música. Pablo Picasso fue un hacker de la pintura. Gari Kaspárov es un hacker del ajedrez. Leonardo da Vinci fue un hacker en varias áreas como por ejemplo la ingeniería. Nikola Tesla fue un hacker de la electricidad. Y la lista sigue y sigue con mucha gente en las más variadas profesiones.

¿Cuál es la diferencia entre el "hacker bueno" y el "hacker malo"?. Para saberlo, hay que responder dos preguntas: ¿qué haces y por qué lo haces?. Los "buenos" se dedican a aprender todo lo que pueden para construir cosas y para arreglar cosas. Los "malos" también aprenden pero para destruir cosas o molestar todo lo que puedan. Cada uno tiene sus motivaciones, sea de los "buenos" o de los "malos". Algunos lo hacen por diversión, otros porque les pagan, otros simplemente "porque si".

Hackstory trata sobre los hackers de la informática, y eso de por si es un campo de acción realmente grande. Sistemas operativos, hardware, telecomunicaciones, inteligencia artificial, malware en sus diferentes formas (virus, gusanos, troyanos, etc.), etc. Yo simplemente voy a escribir, muy por encima, de lo que he conocido a lo largo del tiempo que llevo en esto, y son ya unas cuantas décadas. Hay varios tipos de hackers.

El newbie: es el nuevo o novato. Lo más habitual es que se dediquen a bajar manuales de Internet y, como mucho, siga esos manuales. No suele avanzar más allá de dichos manuales.

El hacker: aprende, aplica lo aprendido y va explorando las diferentes opciones que encuentra. Con el tiempo va aplicando sus conocimientos a sus objetivos. Generalmente solo enseñan las cosas básicas y dan la orientación básica, siendo cada cual el que debe avanzar por si mismo.

El hardware-hacker: se dedica a “trastear” con los diferentes componentes de un ordenador (RAM, CPU, placa base, etc.) analizando las diferentes opciones con el objetivo de sacar el máximo rendimiento al ordenador.

El gurú: es un “hacker especializado” en un tema en concreto, conoce todo lo que hay que saber sobre dicho tema porque se dedica exclusivamente a el.

El “black hat hacker” o hacker de sombrero negro: es un hacker que se dedica a entrar ilegalmente en sistemas, robar información (datos de tarjetas de crédito, por ejemplo), alterar el normal funcionamiento del sistema para perjudicar a los usuarios, dejar el sistema inutilizado, etc.

El samurái: se parecen mucho a los hackers de sombrero negro, pero con una diferencia muy importante: su objetivo es descubrir fallos de seguridad y arreglarlos. En ningún caso buscan perjudicar a los usuarios o al sistema.

Espero que con estas definiciones básicas, cuando leas algo en la prensa sepas mejor de que están hablando realmente.

Altair Div

¿Por qué me enamoré de los hackers?

Fri 25 May 2012 01:06:51 PM CEST

¿Que por qué me enamoré de los hackers? Porque son gente lista y genial, de inacabable curiosidad, sentido del humor y vorazmente críticos, capaces de ponerlo todo patas arriba porque se les ocurrió una idea y con una ética colectiva que está cambiando el mundo. ¡Ah, no! ¿Que no es así como pensabas que eran los hackers? ¿Imaginabas unos tipos malvados, delincuentes habituales, sin empacho en asaltar tu ordenador y tu cuenta bancaria? ¿Esos de los que hablan día sí día también los medios y la policía, poniéndoles la etiqueta de "hacker"?

Bueno, sí, son hackers, si te ciñes a la definición estricta: "Persona que disfruta explorando los detalles de cómo funcionan sistemas, ordenadores y redes, opuesto a la mayoría de usuarios, que prefieren aprender lo mínimo necesario". Sí, todos son expertos en tecnología, pero a los hackers dedicados al Mal la comunidad prefiere llamarlos "hackers de sombrero negro", "hackers malos"... ángeles caídos.

Los hackers que yo amo no matarían una mosca. No te digo que no se hayan divertido alguna vez asaltando un sistema, pero no roban ni destruyen. Curiosean. Avisan de que hay tal problema. Un hacker, dice un amigo, es alguien capaz de encontrar una solución elegante a un problema importante. Eso valoran los hackers. No el dinero que puedan robar. Su tesoro es el conocimiento. Están más allá.

Ellos crearon la red. Crearon los primeros ordenadores, los primeros programas que dieron vida a los ordenadores, las redes y protocolos que los pusieron en contacto. Internet es hija de la comunidad hacker y la forma como está montada, como funciona, transmite su forma de ser. Por eso quien entra, cambia. Mucho o poco, pero cambian sus conexiones neuronales y sociales, se activan ideas y un sentido de la moral que quizás ya tenía, pero estaba durmiendo, sin espacio donde expresarse.

Es por eso que el sistema, ese gigante con pies de barro, ahora hasta el cuello, criminaliza a la comunidad hacker. Sabe que su forma de pensar es su perdición porque es parte del nuevo mundo que vemos eclosionar a nuestro alrededor. Los Indignados no existirían sin Internet. Todos los cambios sociales que estamos viviendo pasan por la red. Ellos, los hackers, la construyeron. Y la gente no hace más que ser digna de este legado.

La comunidad hacker tiene una ética comúnmente aceptada que dice cosas como las siguientes: "El acceso a los ordenadores y a todo lo que te pueda enseñar alguna cosa sobre cómo funciona el mundo debe ser ilimitado y total". "Toda la información debería ser libre". "No creas a la autoridad, promueve la descentralización". ¿Qué, te gustan? ¡A ver si tú también te habrás enamorad@ de los hackers!

Mercè Molist Ferrer. Fundadora de Hackstory.net

Texto publicado en el diario “El Mundo”, en el contexto de la promoción de la campaña de crowdfunding que se llevó a cabo en junio y julio de 2012. El objetivo era conseguir dinero para pagar el tiempo de escribir este libro que tienes ante tus ojos.

La campaña se realizó en la plataforma Goteo y superó todas las expectativas, llegando a recaudar 6.000 euros, donados por 131 personas, la gran mayoría pertenecientes a la comunidad hacker hispana.

Gracias

A Manuel Medina, que me animó. A Adrià García, que me enseñó qué es un hacker. A Luis García-Rosales, Jordi Linares y Jordi Murgó, mis tutores en el “under” y, los dos Jordis, inventores del título de este libro. A Vins Vilaplana y Claudio Hernández, que tuvieron la paciencia de leer la versión (extended) y aportar mejoras. A Roberto Macías, que me acompañó hasta el final, y Altair Div, que siempre está ahí. A Cyteck (Gerard Romans) que diseñó las camisetas y la portada del libro. A Rocío, que diseñó el libro. A Xavi Caballé, Blackhold (Laura Mora), Miguel García LaFuente y Jay Govind, que aportaron su saber técnico. A Sergio Solís, que creó el blog de Hackstory, y Alan Lazalde, que abrió @hackstory_ en Twitter. A Albert StateX que cogió el testigo de la cuenta en Twitter y sin cuya ayuda no habríamos vendido ni una camiseta en la No cON Name. A Mónica Lameiro que co-administró el grupo Hackstory en Facebook. A María Laura Quiñones Urquiza, nuestro contacto con Latinoamérica. A Karma Peiró, que estuvo ahí. A José Luís Verdeguer, Antonio Martín y Jericho. A Enric Senabre, de Goteo. A la gente que donó su dinero en la campaña de crowdfunding, a l@s amigos periodistas que hicieron correr la voz, a Chema Alonso y Nico Castellano, que pusieron sus negocios al servicio de Hackstory. A la lista Pléyade. A los foros Hackstory y EX IRC-Hispano. A la gente de Twitter. A la Wikipedia.

A Alfonso, mi hacker de guardia. A Bet, que tuvo paciencia mientras mamá escribía el libro.

Y a vosotr@s, tras vuestras máscaras, o sin ellas, que desde los confines del ciberespacio me enseñasteis. Gracias.

Las cosas claras

Hola, soy morgana. Y M&M. Y merce. Maria Mercè Molist i Ferrer, una chica de pueblo que en 1995 entró en Internet.

No he escrito este libro para ti. Lo he escrito para mí. Para mi curiosidad, mi placer al investigar, mi diversión de escribir. Y lo he escrito para ellos. Los hackers. Para que no se olviden sus nicks, sus hazañas y sus retos.

Ten siempre presente cuando lo leas, como yo lo he tenido al escribirlo, que este libro no es todo lo que fue. Es, como explica el wiki que le fue origen, Hackstory.net *"lo que sabemos sobre la historia de los hackers"*. Lo que nos han dejado saber.

Si no eres uno de ellos, o no viviste en la Internet de los años 90, te recomiendo leer el siguiente glosario. Sí, ya sé que nadie lee los glosarios. Pero no voy a bajar el nivel a media historia para explicar cosas que deberían estar entendidas. Así que, como te diría un hacker: Read The Fucking Manual!

Jargon

BBS

Siglas de Bulletin Board System. Las BBS nacieron en los 80-90. Consistían en un ordenador y uno o más módems, usualmente en la habitación de un chaval. Se llamaba al módem para entrar dentro, donde había programas, textos, warez y foros.

Chat

Un canal de chat es una zona de charla mediante texto donde la comunicación es instantánea.

Deface

Defacement es entrar sin autorización en un servidor web y dejar un mensaje en la portada.

Grupo de noticias

Nacieron en 1979 y eran muy parecidos a los foros en la web, pero su base no era la web sino la interconexión de miles de servidores en todo el mundo.

Lista de distribución de correo electrónico

Foro basado en el correo electrónico, es la forma de comunicación colectiva más antigua de Internet. Los mensajes de los contertulios se reciben en el propio buzón de correo.

Servidor

Normalmente es un ordenador que da servicios a personas, programas u otros ordenadores, llamados *clientes*. Por ejemplo, un servidor web sirve páginas web a los usuarios.

Software libre

Programa que garantiza las libertades de:

0. Usarlo con cualquier propósito.
1. Estudiar cómo funciona y adaptarlo a las necesidades propias, accediendo al código fuente.
2. Distribuir copias del programa.
3. Mejorarlo y hacer públicas las mejoras.

Warez

Programas “pirata”, a los que se han quitado las protecciones anticopia sin autorización de sus creadores.

Ética hacker

Hackers y consciencia ética son términos indivisibles desde la primera red, ArpaNet, donde se discutían con pasión los buenos y malos usos de la tecnología. Esta ética es el punto de unión, en forma de nebulosa de ideas compartidas, de la comunidad hacker del planeta.

CAPÍTULO UNO

Prehistoria

Prehistoria

Miquel Barceló, escritor y profesor de la Universitat Politècnica de Catalunya (UPC), suele contar que los primeros hackers... ¡no sabían que eran hackers!. Más bien se les consideraba *chalados de la informática*. La palabra hacker se inventó en los años 60 en una universidad norteamericana, el Massachusetts Institute of Technology (MIT), y tuvo que pasar un tiempo, un buen par de décadas, hasta que se difundió más allá de aquel país.

Pero, se les llamase como se les llamase, está claro que los primeros hackers nacieron con los ordenadores, que aparecieron en universidades y empresas en los años 60, 70 y 80, más pronto o tarde según se viviese en uno u otro lado del charco y más al Sur o más al Norte. Eran unos pocos privilegiados quienes podían interactuar con esas máquinas, primero inmensas y progresivamente más pequeñas. De ellos, sólo algunos se lo tomaron como algo más que un trabajo y cayeron rendidos al hechizo de la máquina: esos fueron los primeros hackers, mentes curiosas que querían saber cómo funcionaban los ordenadores, cómo construir programas que les diesen vida y redes que uniesen sus destinos.

Quien llevaba la delantera en esta aventura era Estados Unidos, que en 1969 ya estaba creando la red ArpaNet, llamada comúnmente *la madre de Internet*. Fue entonces, a finales de los 60, cuando llegaron a algunas universidades norteamericanas los legendarios PDP, los primeros ordenadores que no necesitaban una habitación para ellos solos y que los alumnos podían tocar. Así nacieron los primeros hackers: los hackers del MIT.

Por cierto que la palabra *hacker* no se inventó en un sala de ordenadores sino en un club universitario de aficionados a las maquetas de trenes, el Tech Model Railroad Club: sus miembros acostumbraban a llamar hacker a quien solucionaba de forma elegante algún problema ferroviario. Y, como la mayoría de socios del club se volcaron en los nuevos PDP, de forma natural su jerga se trasladó a la nueva vida con el ordenador.

Podríamos estar horas hablando de aquellos primeros hackers, de sus noches de pizza y café en la universidad, creando los primeros juegos, como Spacewar!, los primeros programas, la primera ética hacker, en un ambiente lúdico, entre genios. Pero ya hay libros que lo cuentan. Uno de los mejores: Hackers, heroes of the computer revolution, de Steven Levy.

Levy habla en su libro de tres generaciones de hackers: los *auténticos* ("true hackers"), quienes en los años 60, desde universidades como el MIT construyeron los primeros programas y crearon la *way-of-life* hacker. Los "hardware hackers", que en la década de los 70, en California, construyeron los primeros ordenadores personales, las primeras bluebox y las primeras BBS. Y los "game hackers", en los 80, los programadores de la industria del videojuego.

En Europa, estas tres generaciones fueron una, pues ni había tanta gente, ni tanto

ordenador, ni tanta industria. Todo o casi todo venía de Estados Unidos y era impepinable que, si alguien quería meterse a hacker, debía entender inglés pues todos los manuales, sistemas operativos, lenguajes informáticos, estaban en este idioma. De aquí la importancia de las traducciones, algo en lo que se volcarían muchos hackers europeos en los 90... pero esta historia se contará más adelante.

En España, en los años 70, los hackers eran cuatro gatos. En 1985, los centros de cálculo de cada universidad no tenían más de 2, máximo 3 ordenadores, según el Estado de Situación Proyecto IRIS, recuperado gracias a Francisco Montserrat, de IRIS-CERT. La cosa no estaba mejor en las empresas, pues sólo las grandes tenían ordenadores.

Quienes los manejaban eran ingenieros, como Miquel Barceló. O viejos lobos autodidactas, como Alberto Lozano. O becarios, como Martí Griera, que fue justo acabar la carrera y ponerse a montar redes pan-europeas. Sin manual de instrucciones, descifrando conceptos tan complejos que nadie más manejaba en su entorno, es una pena que muchos de aquellos geniales pioneros simplemente han sido olvidados.

Queda el recuerdo en los documentos oficiales para quienes tenían responsabilidad: Víctor Marquès y Miguel Ángel Campos en la Universitat de Barcelona, José Miguel Femenia y Rogelio Montañana en la Universitat de València, Miquel Àngel Lagunas y Manel Marín en la Universitat Politècnica de Catalunya, Jordi Adell y Toni Bellver en la Universitat de Castelló, José Antonio Mañas en la Universidad del País Vasco y después, la Politécnica de Madrid, José Ramón Martínez Benito y Josu Aramberri en la Universidad del País Vasco, Iñaki Martínez y Miguel Ángel Sanz en RedIRIS **[1]**... La mayoría jamás medraron, construyeron en un esfuerzo épico la red y después volvieron a sus trabajos de profesores.

Junto a ellos, a principios de los 80, otro tipo de hackers: los programadores que se volcaron en la exitosa industria española del videojuego. Cabe aclarar que de aquellos hackers *jugones* se ha escrito lo suficiente para que no sea necesario que este libro abunde más en ello. A quien tenga curiosidad le remitimos al excelente artículo sobre la Historia de los videojuegos de la Wikipedia. Y a la serie La edad de oro del software español del blog Insert Coin. De esta serie, Hackstory.net ha replicado los artículos que versan sobre las empresas Dinamic, Aventuras AD, Opera Soft, Topo Soft y Zigurat.

Todos ellos, investigadores de las universidades, de las empresas y del videojuego, son los dinosaurios que formaron la primera generación de hackers en la Península Ibérica. Aunque, como dice Barceló, no supiesen hasta muchos años después que lo eran ;)

1. Miquel Barceló

Miquel Barceló nació en Mataró (Barcelona) en 1948 y es catedrático del departamento de Lenguajes y Sistemas Informáticos de la Universitat Politècnica de Catalunya, amén de un reconocido aficionado a la ciencia ficción. Barceló fue uno de los primigenios hackers españoles.



Miquel Barceló fotografiado por SINC

1.1. De becario con los primeros ordenadores

Estudió en la Escuela de Ingeniería Aeronáutica de la Universidad Politécnica de Madrid (UPM), donde se sacó el título de ingeniero aeronáutico en 1970. Empezó a tocar ordenadores en 1968, en la UPM. Durante el curso 70-71 trabajó en el Centro de Cálculo de la UPM y, a la vez, en los ordenadores de la Junta de Energía Nuclear.

> En la Escuela de Ingeniería Aeronáutica teníamos un profesor de matemáticas que estaba en una empresa, Conducciones Aeronáuticas, y era uno de los pocos usuarios que había a finales de los 60 de un 1401 de IBM. A los que éramos buenos en mates, que éramos un par, nos dejaba hacer programas con una calculadora Olivetti que compró. Era una época muy romántica, porque había pocos ordenadores, y también divertida: para enseñar su máquina a los clientes, IBM tenía un avión con la máquina dentro. Lo aparcaba una semana en el aeropuerto de Barcelona e invitaba a grandes empresas a verlo. En el último año de carrera fui becario de Iberia, que en el 69-70 ya tenían ordenadores, y tenían un 360 de IBM. Vimos una demostración del sistema 3 que nos hicieron desde Roma con una terminal en Madrid.**[2]**

Barceló recuerda su paso por la Junta de Energía Nuclear con cierto escalofrío:

> Tenían una *Sperry Rand*, que era la marca grande que cubría Univac. Iba con tarjetas, tenía 5 Ks y era tan pequeña que el compilador FORTRAN se tenía que entrar en tres trozos. Hice algún programa para esta máquina cuando estudiaba ingeniería nuclear, de control de seguridad de núcleos. Pero acabé largándome porque pensé: si la seguridad nuclear de este país se hace así, apaga y vámonos.**[3]**

1.2. El hacking como diversión... en Bull

Después de doctorarse en Italia, volvió a España y empezó a trabajar en la incipiente informática comercial.

> Hacíamos programas en Cobol, aplicaciones... Los vendedores vendían la máquina a grandes empresas que usaban los ordenadores para la contabilidad, facturaciones, nóminas, bancos y cajas que hacían transacciones...; les regalaban los cursos de formación, el software y tantas horas de un ingeniero de sistemas que les ayudase a montar aplicaciones. Yo hacía este tipo de cosas.**[4]**

Pero Barceló nunca fue un gris obrero de la informática: él era un hacker o, como explica, un loco de la informática.

> Yo era un loco de esos que les gusta saber más cosas de las que hay que saber. Si a un tío se le rompía un disco y de 10 megas podía salvarle 9 y media, pues todo eso que le había salvado. Esto significaba hacer programas directos con ensamblador, acceder físicamente al disco, rastrear en el disco dónde están los bloques de información del fichero, irlos buscando.**[5]**

Cabe recordar que en aquella época no se hablaba de hackers, ni en la prensa ni en los círculos informáticos, pues no se conocía tal palabra. Barceló era, para sus colegas, uno que hacía "chorradas":

> Yo era capaz de hacer cosas que mis compañeros no hacían y lo consideraban una chorrada, pero yo me divertía haciéndolo, con unos programas que eran como unas pinzas, reconstruyendo información y montándola en otro disco.
>
> Por ejemplo, uno de los primeros programas comerciales que hice, en Bull, para gestión de "stocks". Lo hice con una máquina de 5 Ks de memoria. Lo lanzamos a las 9 de la mañana y a la 1 teníamos que ir a comer y no acababa. Todos hacían broma diciendo que se había metido en un bucle.
>
> Lo cerré y, antes de ir a comer, hice una modificación para que cada registro que tratase pusiese 1, 2, 3, 4, 5, 6, 7, 8. Lo pongo a funcionar, me voy a comer. 1.200 y el programa continuaba: ¡duraba 3 horas y 40 minutos!. Como los programas no tenían para hacerles el seguimiento, se me ocurrió usar un visor como control de mantenimiento, para que hiciese de contador, programarlo en ensamblador y hacer visible que el programa tiraba para adelante, pues con aquellas máquinas era todo muy lento.
>
> Este tipo de cosas, había gente que les hacía ilusión hacerlas y otros que pasaban, incluso algunos me reñían. Es hacer una cosa no habitual porque te apetece.**[6]**

Sea como sea, las "chorradas" de Barceló y de tantos otros hackers habían salvado a más de uno, incluida la Compañía Telefónica Nacional de España cuando instalaba sus primeros nodos X25:

> En el año 80 estuve con una máquina que se llamaba *Nivel 6*, una máquina de comunicaciones. Cuando los de Telefónica pusieron el primer X.25 había unos paquetes que había que contar de forma decreciente desde 64.000 o cuando empezases y Telefónica los contaba al revés. No les funcionaba, claro, hasta que les hice notar que el orden debía ser decreciente, no creciente.**[7]**

Barceló trabajó como ingeniero de sistemas de Bull España desde 1972 a 1989. Entre muchos recuerdos, aún sonríe cuando piensa en un ordenador de esta empresa, llamado *G-58*, una máquina pequeña, con una versión de 5 Ks de memoria y otra de 10, con la que se divertían además de trabajar:

> Teníamos un programa que lo ponías a rodar y hacía un bucle. Entonces, cogías un transistor cualquiera, lo acercabas a la unidad central de memoria y las interferencias radiológicas que salían de los circuitos de la máquina hacían sonar La Marsellesa. El *G-58* no tenía juegos, pero los hacíamos nosotros. Esto era el hacking a principios de los años 70, el hacker que sabía más informática de lo habitual y hacía cosas insospechadas. Era un hacking muy inocente, sin mala baba.**[8]**

Había más ocasiones para exhibir el espíritu humorístico de aquellos primigenios hackers. Barceló recuerda, en el Centro de Cálculo de la UPM, su actividad diaria de cada mañana: cargar en la impresora un programa, regalo del CERN (Organización Europea para la Investigación Nuclear), quien había vendido la máquina al centro. El programa hacía que los golpes de martillo de la impresora entonasen el himno norteamericano "Barras y estrellas". Otra diversión con las impresoras era crear programas que hacían dibujos con sólo mayúsculas y gradaciones de negro, uno de los más típicos era un cristo crucificado. Podría considerarse el antecedente más directo del arte ASCII.

1.3. El nacimiento del hacking para todos

El hacking de entonces se hacía con sistemas propietarios y en ámbitos muy cerrados, de empresas para las que el conocimiento era dinero:

> El conocimiento técnico del informático de la empresa era pequeño, mientras que el del técnico de IBM era más alto. Seguramente no tanto como los que habían fabricado el software, pero al menos tenía acceso a él. Por tanto, el único que podía ser hacker era el técnico de IBM, pero a este no le interesaba ser hacker en el sentido de reventar el sistema que le daba de comer.**[9]**

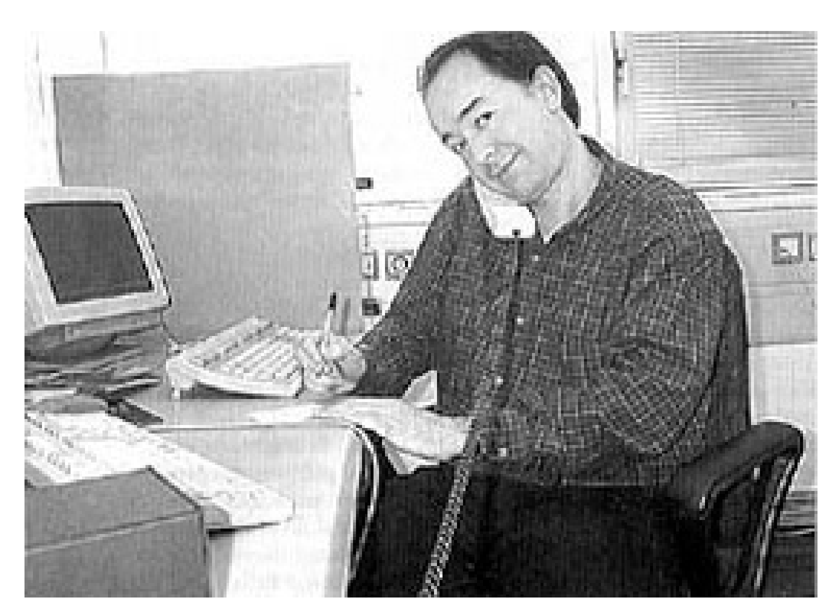
Hasta que el conocimiento no salió de aquellos santuarios, no puedo nacer el hacking como tal:

> En el momento que el conocimiento técnico se va generalizando, y esto pasa con los PDP y VAX de Digital, que son máquinas que están en las universidades, mucha gente conoce las tripas y cómo funcionan. Y después las máquinas con sistema operativo Unix.
>
> Estas máquinas empiezan a tener un sistema operativo y herramientas, el conocimiento de los cuales ya no es sólo propiedad de Digital sino de todos los profesores y estudiantes universitarios. Esto hace que empiece a haber un montón de gente que sabe cosas, y nace el hacking a gran escala. No hay nadie que haga hacking de un gran sistema de IBM porque muy poca gente conoce los intríngulis de este sistema. ¿Has oído hablar alguna vez de un virus de un *AS400* de IBM? ¡Porque nadie lo conoce!. El hacking que se hace famoso es en las

universidades, a partir de los PDP, VAX y máquinas UNIX, en los años 80. Y, a partir de los 90, con Internet y Windows.**[10]**

2. Martí Griera

Cuando empezó a trabajar en la universidad, Barceló encontró a hackers como Martí Griera, hoy responsable de redes en la Autònoma de Barcelona (UAB). Griera entró en los servicios informáticos de esta universidad cuando acabó la carrera, en 1985, a las órdenes de Llorenç Guilera, quien fue el primer director del servicio informático de la UAB.



Martí Griera en el 2000, por Victor Colomer

2.1. El correo electrónico mueve montañas

Griera trabajaba en sistemas. Sólo tenían un servidor, una única máquina, y pocos terminales. Era una estructura radial formada por VAXes. La UAB fue la primera universidad española en usar estos ordenadores, desde 1980.

En 1986 se tiró una red Ethernet por todo el campus. Iba a 10 Megabits y los módems, a 300 bits por segundo. Las terminales se conectaban al servidor a 1200 bits por segundo. Era una red de poca capacidad, pero tampoco se necesitaba más ya que la capacidad de generar tráfico era baja.

Había más usuarios que terminales (40), lo que obligaba a trabajar por turnos. Los estudiantes tenían los horarios más malos. Desde el terminal se podían correr básicamente aplicaciones de gestión: nóminas, matrículas, gestión de la universidad, administración, contabilidad. Los profesores lo usaban para aplicaciones técnicas de cálculo y para el correo electrónico en modo local, el servicio con más éxito.

> El siguiente paso fue decir: me gustaría intercambiar correo con gente de la Universidad de Barcelona (UB). Para eso necesitábamos un cable entre nosotros y la UB, conectarnos a la red de Telefónica o montarnos una línea telefónica y hacer la red. El correo fue la razón de conectarnos.**[11]**

2.2. Las primeras redes eran P2P

A finales de los 80, la Universitat de Barcelona (UB) era la más interconectada con

otros universidades españolas. Miguel Ángel Campos, responsable de los servicios informáticos, llevaba también el nodo de la red EARN (European Academic and Research Network) en la UB.

EARN había sido promovida y financiada por IBM. Era la versión europea de la estadounidense BITNET a la que pertenecían las universidades americanas, y de hecho estaba integrada en BITNET. La mayoría de universidades europeas estaban conectadas a EARN.

> En 1984 conectaba ordenadores de distintos tipos entre 22 países, entre ellos la Universidad de Barcelona y las universidades Autónoma y Politécnica de Madrid. (...) A principios de los 90 EARN llegó a conectar en España cerca de 40 ordenadores de unos veinte centros de cálculo de universidades y organismos de investigación.**[12]**

Tanto EARN -que moriría en 1992- como BITNET eran redes de peers o iguales, algo que marcó para siempre a los hackers que, como Martí Griera, las construyeron:

> Se llamaban *peering networks* porque, a diferencia de las redes de Telefónica, donde tenías el terminal, eran redes entre iguales, todos teníamos nuestro ordenador y nos pasábamos información. El *peer-to-peer* (P2P) es el origen de Internet, conectar máquinas iguales.**[13]**



Iberpac en 1985, según el Documento original del proyecto que dio lugar al RedIRIS

La estructura de Internet en aquellos momentos era tan sencilla que podía explicarse en un libro, donde todos los dominios y direcciones de correo cabían en un anexo del mismo.

> En los Estados Unidos había universidades que tenían contratos con el Departamento de Defensa y montaron una red TCP/IP, que es el núcleo de Internet. Las que no tenían contratos con Defensa montaron BITNET para intercambiar correo electrónico con todo el mundo a través de pasarelas y, más adelante, grupos de noticias. En algunos sitios había conexiones estables, mientras que en otros alguien de la universidad se conectaba para bajarse el correo y después cerraba**[14]**

Por otro lado, estaban las redes X.25 de las compañías telefónicas. Iberpac era la

red X25 de la española Telefónica, que fue pionera en este tipo de redes desde los años 70, el usuario sólo tenía acceso a un terminal de la red, de forma que Telefónica mantenía el control de la estructura y el cliente no sabía qué había dentro ni podía manipularlo.

2.4. No fiarse de Telefónica

Para aquellos primeros hackers de las universidades, acostumbrados a trabajar en abierto, el invento de las compañías telefónicas no sonaba nada bien, así que actuaron en consecuencia, explica Griera:

> La gran revolución, el cambio de chip llega cuando no me fío de las telefónicas ni les doy la inteligencia a ellas. Ya que mis ordenadores son de propósito general y potentes, haré que mi ordenador sea un nodo de la red y a Telefónica le compraré líneas punto a punto para crear esa red, pero no sabrá qué hay dentro ni que hemos hecho una red. Y la hemos podido montar porque no lo saben. Si lo hubiesen sabido se lo habrían cargado de entrada.
>
> Recuerdo cuando montábamos los primeros módems. Te ponían un módem de 300 bps y si querías uno de 1200 tenías que pagar 4 veces más. Todo era super caro, no podías montar una línea con dos módems que no fuesen de Telefónica, era ilegal. Pero la primera línea que tuvimos con EARN era de 1200 bps, para pasar todo el correo de la universidad, así que tuvimos que montar cosas ilegales: teníamos una sucursal de la universidad en Girona, quitamos los módems de Telefónica y montamos otros más rápidos. Y nos costaba exactamente igual que con Telefónica.
>
> El cambio de concepto, revolucionario, es decir: no me fío de esa gente y monto una estructura donde los nodos de la red no me los ponen ellos sino que los pongo yo y a ellos sólo les compro lo indispensable: los cables.**[15]**

2.5. RedIRIS

Paralelamente, a mediados de los 80 empezó la creación y despliegue de RedIRIS, la Red para la Interconexión de los Recursos Informáticos, destinada a universidades y centros de investigación. Pero su forma de funcionar no gustó a todos, ya que se basaba en X25 y apostaba por la tecnología OSI en detrimento de TCP/IP.

> Durante muchos años RedIRIS estuvo con x400, tecnologías OSI. Hay que decir en su descargo que en aquel momento los fondos europeos querían potenciar OSI frente al modelo IP, que se veía muy americano. Seguíamos un esquema de dependencias, de subsidios, no teníamos iniciativa porque teníamos los subsidios de Madrid, que vivían de los subsidios de Europa y alguien en un turbio despacho dominado por las telefónicas europeas, que no querían que el negocio se les escapase de las manos, decía: OSI, porque así tendremos el negocio bien atado. No había ningún tipo de criterio.**[16]**

Además, explica Griera, era una red montada a golpe de talonario por Telefónica:

> RedIRIS llegó con la tira de pasta. Nacía de Fundesco, una fundación de Telefónica, que puso a sus esbirros al lado del poder para montar RedIRIS y destrozar lo que estábamos haciendo. Se montaron cosas demenciales: redes con unas facturas de medio millón de pesetas por tener un enlace entre nosotros y Madrid, porque cada bit que pasaba Telefónica lo cobraba. Entonces vieron que no podían seguir así, era tan descarado que no podían ni pagar las

facturas, y dijeron: montaremos nuestra red, con líneas punto a punto, pero con x25 por encima, y montaron Artix. La UAB no se apuntó a eso porque decíamos que era una cutrada. Y el tiempo nos dio la razón.**[17]**

3. Alberto Lozano

Alberto Lozano es consultor tecnológico desde 1984 y gurú de la comunidad *maquera* española. Nació en Santa Coloma de Gramenet (Barcelona) el 21 de enero de 1947. Su trayectoria le acerca mucho a la siguiente generación de hackers, de los que podría considerarse la avanzadilla.



Lozano, a la derecha, con unos amigos en la calçotada de 2006

3.1. Un enamorado de la electrónica

Lozano estudió en la Escuela de Peritos Industriales de Barcelona y a los 18 años creó su propio negocio de reparación de televisores y diseño y montaje de emisoras de radio. En 1969 entró en la empresa Gispert (Philips) como reparador de calculadoras digitales electrónicas y, posteriormente, jefe de laboratorio. Después en otra empresa diseñó los primeros aparatos, tan populares en las tiendas, "Su turno":

> Una empresa italiana hacía unos trastos que valían una burrada y una empresa de aquí me pidió hacerlo más sencillo. Yo venía de diseñar calculadoras y pensé: ostras, si esto es una cosa de numerar con un display. Pues no hagamos un circuito de electrónica increíble, cojamos un chip de calculadora, que valía 500 pelas, un circuito que cuando pulses la tecla haga 1+ automáticamente y unos amplificadores para hacer los números grandes. Así hicimos, con un coste mínimo, los primeros "Su turno".**[18]**

En 1972 se estableció como consultor de electrónica digital. Entre sus proyectos de aquella época destaca el diseño de la primera calculadora de bolsillo fabricada en

España.

> -Porque tú empezaste con la electrónica…
>
> -Sí, soy electrónico. Cuando tenía 18 años estudiaba, más o menos, porque me cansaban los estudios, y me ganaba la vida reparando televisores. Tengo un laboratorio en el garaje de casa.
>
> -¿Y qué haces?
>
> -Si algo se rompe, lo reparo. Cuando digo reparo me refiero a la placa, no la cambio, por puro hobby. Reconstruyo radios antiguas, tengo una colección de los años 50-60 funcionando perfectamente. Es compulsivo: cada vez que llega algo electrónico, sobre todo antiguo, ponerlo en marcha. He diseñado el sistema de seguridad de mi casa, cámaras y todo. Tiene una ventaja: los ladrones no lo revientan porque no es estándar, no está en los catálogos y no saben qué hacer.**[19]**

3.2. ...y un enamorado de Apple

A mediados de los 70, la aparición del primer ordenador de Apple y la admiración que sintió Lozano por este dirigieron su curiosidad personal y profesional hacia la informática personal. Compró uno de los primeros Apple I y, en 1976, un Apple II.

> El primer ordenador personal serio de la historia fue el Apple II. Entró directamente en mi vida por dos razones: La primera es que yo tenía ya un ordenador personal construido y diseñado por mí (en base a un procesador de cuatro bits SC/MP de la National) pero que no tenía ni punto de comparación con el Apple II. La segunda es que el Apple II venía con todos los esquemas y con notas manuscritas de su diseñador, Wozniak, un tío c*j*n*d* donde los haya. Conocí a Wozniak y a Jobs en persona y eran unos tíos increíbles.**[20]**

Lozano no sólo tuvo en sus manos los primeros Apple, sino que también ayudó a fabricar sus primeros clónicos:

> El Unitron, la ROM era mía. Los hacía una empresa de Barcelona y no los podía vender porqué había dos ROMs con copyright de Apple. Me dijeron: Haz que funcione sin que la ROM sea igual. Cifré el contenido de la ROM e hice una rutina que, cuando encendías el Unitron, descifraba y en RAM te hacía una copia de ROM que era la de Apple. Pero, cuando apagabas la máquina, aquello se esfumaba. Si un juez cogía la ROM y la leía, no se parecía en nada a lo de Apple. O sea, no diseñé una BIOS, hice la misma, cifrada. Fue un hack: una solución interesante a un problema importante.**[21]**

En 1978, puso en marcha el primer club de usuarios de ordenadores personales en España, dedicado a los propietarios de Apple II, *Pet* de Commodore y *TRS-80* de Radio Shack. El club se llamó *Run* y llegó a tener 100 socios. También montó junto a un socio la primera tienda de ordenadores personales de España: Isecom SA.

En 1987, Edica (Editorial Católica) le encargó montar el sistema redaccional y de fotocomposición del diario “Hoy” de Badajoz con Macintosh.

> Como consecuencia del montaje del “Hoy”, fui conocido en el mundillo de la prensa y comencé a asesorar a otros periódicos que se pasaron a Mac. Diseñé la red del extinto “Sol” de Madrid, la del “Sport” de Barcelona, La de “Informacions Diari de Andorra”, “Prensa de Ibiza”, etc.**[22]**

3.3. De Solo Mac a Seker, pasando por Servicom

En 1985 montó la BBS *Mac Help*, que posteriormente se llamaría Solo Mac. Lozano la concebía como su "sistema de telecomunicaciones de atención a clientes"**[23]** pero en 1992, cuando ya tenía 600 usuarios, la abrió al público y la conectó a Internet.

> Hice un proyecto para la Diputación de Vitoria que consistía en montar una estación meteorológica en cada valle, intercomunicadas por módem. Un meteorólogo recogía toda la información y la enviaba a los ayuntamientos, para que los ganaderos supiesen el día anterior si podían sacar las vacas o no. Año 85. Yo vivía allí, en un pueblo, y monté Mac Help. A veces, llamaba alguien y me decía: oye, que no contesta la BBS. Bajaba a la caseta de Telefónica, que estaba en la carretera, le daba un par de patadas y funcionaba.**[24]**

En 1993 conoció a Eudald Domènech, con quien montaría uno de los primeros proveedores de acceso a Internet comerciales en España, Servicom:

> Vine a vivir a Taradell (Barcelona) y, en un encuentro, la Semana Santa del 93, monté una red en el ayuntamiento conectada por módem, para mostrar a la gente cómo era. Durante los 3 días que duró, había un tío en el fondo de la sala de actos mirando todo el rato. Al tercer día viene y me dice: Me llamo Eudald Domènech, creo que esto es el futuro, tú tienes aquí 300 usuarios, vamos a hacer un negocio de 300.000. Así nació Servicom.**[25]**

Pero la entente Lozano-Domènech duró poco. Un año después el primero abandonaba Servicom:

> Servicom fue una gran inversión en publicidad y una menos importante en recursos técnicos. Hasta el primero de Agosto de 1994, el centro de comunicaciones de Servicom estuvo en mi despacho particular de Taradell. Para entonces ya me había convencido de que el camino emprendido por Servicom era divergente de mis ideas sobre las comunicaciones y, sobre todo, siendo yo una persona con un espíritu eminentemente técnico, no encajaba con un sistema en el que todos los recursos se dedicaban a la promoción comercial anunciando características que en aquellos momentos los ordenadores de que disponíamos no podían cumplir y sin presupuesto para adquirir nuevo material. De modo que decidí apartarme del proyecto Servicom y reanudar lo que había sido Solo Mac un par de años antes.**[26]**

Lozano abrió otro proveedor, Seker, que abandonó en 1997. Un año después, la empresa se vendió a Primus Tel. por 400 millones de pesetas. Actualmente, Lozano trabaja como consultor tecnológico por su cuenta.

También en 1997, Lozano abrió Los foros de Mac-Club, con cuyos usuarios monta encuentros gastronómicos anuales, cuyo plato fuerte es una calçotada. Esta tradición se inició con la BBS Mac Help, en 1985.

4. Notas

1. ↑ Análisis Histórico de Internet en España (94-02). *Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet. Andreu Veà Baró. Tesis Doctoral (12-09-02)*
2. ↑ Conversación privada con Miquel Barceló
3. ↑ Conversación privada con Miquel Barceló
4. ↑ Conversación privada con Miquel Barceló
5. ↑ Conversación privada con Miquel Barceló
6. ↑ Conversación privada con Miquel Barceló
7. ↑ Conversación privada con Miquel Barceló
8. ↑ Conversación privada con Miquel Barceló
9. ↑ Conversación privada con Miquel Barceló
10. ↑ Conversación privada con Miquel Barceló
11. ↑ Martí Griera, en conversación privada
12. ↑ Las primeras redes: Redes académicas y de investigación. Internet en España, Internet en el Mundo. Asociación de Usuarios de Internet
13. ↑ Martí Griera, en conversación privada
14. ↑ Martí Griera, en conversación privada
15. ↑ Martí Griera, en conversación privada
16. ↑ Martí Griera, en conversación privada
17. ↑ Martí Griera, en conversación privada
18. ↑ Alberto Lozano: hard hard hacker. Revista @rroba, 105 (05/06)
19. ↑ Alberto Lozano: hard hard hacker. Revista @rroba, 105 (05/06)
20. ↑ Personal. Notas de Alberto
21. ↑ Personal. Notas de Alberto
22. ↑ Personal. Notas de Alberto
23. ↑ Personal. Notas de Alberto
24. ↑ Alberto Lozano: hard hard hacker. Revista @rroba, 105 (05/06)
25. ↑ Alberto Lozano: hard hard hacker. Revista @rroba, 105 (05/06)
26. ↑ Personal. Notas de Alberto

5. Enlaces externos

Historia de un Viejo Informático.

5.1. Miquel Barceló

· Miquel Barceló. Es.Wikipedia.

5.2. Martí Griera

· Martí Griera: historia de la @rrob@. Víctor Colomer. Cara a cara. (23-03-00)
· Todo lo que usted quería saber sobre RedIRIS. Tomàs Baiget. “El profesional de la información” (06-92)
· Evolución de Internet en España. Raúl Rivero. Máster de periodismo “El Mundo.
· IRIS-NEWS: la aventura de La Usenet en RedIRIS. Juan Antonio García. Innosec.

5.3. Alberto Lozano

· Notas de Alberto. Web personal de Alberto Lozano.

CAPÍTULO DOS

Los primeros grupos de hackers

Los primeros grupos de hackers

En las universidades estaban pues las máquinas, las redes y buena parte de la primera generación de hackers, aquellos profesores, becarios, investigadores y personal administrativo extremadamente comprometidos con una revolución que no sólo estaban viviendo, sino construyendo con sus propias manos.

Pero, sin desmerecerlos, eran hackers que cobraban por su trabajo y no tenían que preocuparse de pagar las máquinas o la conexión. Hackers de guante blanco, difícil distinguir en ellos la fina línea entre el científico y el hacker.

Los alumnos de las universidades jugaban en otra liga: el acceso a ordenadores y redes para el alumnado en general no llegaría hasta los 90. Así que, si alguien quería ver cómo funcionaba un servidor o mandar un correo electrónico en los 80, tenía que formar parte de la jerarquía de becarios y profesores, o entrar por el otro lado.

Esos que entraron por el otro lado son la segunda generación de hackers, los chavales de la calle, hijos de la revolución de las consolas, que anhelaban tocar las máquinas y pasearse por las redes propiedad de empresas y universidades. Hackers de noche, adolescentes de día, muchos no llegaban a los 20 años. Herederos directos de los *hardware hackers* que había construido sus propios ordenadores, como Alberto Lozano. Son los chicos del Spectrum, de las BBS, los videojuegos pirateados, los chavales que vieron la película Juegos de Guerra (Wargames) a mediados de los 80 y quedaron impactados.

Algunos fueron por libre, pero eran tan pocos aquellos nuevos chalados, ya no sólo de la informática sino también las redes, que la evolución natural les llevó a unirse en grupos, los primeros grupos de hackers, pequeñas tribus donde podían reconocerse y apoyarse en el otro, algo esencial cuando se tiene una afición tan minoritaria y aislada socialmente. Grupos donde echarse unas risas, donde presumir de las hazañas que nadie más entenderá y, lo más vital, donde intercambiar información y aprender para seguir avanzando en la afición... o adicción.

Y así como los primeros hackers que, teniendo ante sí una máquina, construyeron programas para darle vida, aquellos hackers de barrio, la segunda generación, crearían los primeros sitios de reunión, las BBS, y los programas para conectar sus consolas a ellas. Y, si el programa ya existía pero era de pago... no dudarían en piratearlo.

> La gente de mi generación, que ha seguido a ritmo constante, tiene historias muy similares. Somos hackers por necesidad, la informática de la época era escasa y cara y tenías que buscarte la vida para tener herramientas, información, acceder a redes, investigar como funcionaban… para hacer los programas que te evitarían el pago.**[1]**



Hubo un tiempo en que Internet era solamente un lugar para los supervivientes, un tiempo en el que el conocimiento se adquiría a base de mucho trabajo personal.

Un tiempo en el que el respeto se ganaba compartiendo con los que no sabían aquellas cosas que habías aprendido con esfuerzo.

Un tiempo en que la tecnología dejaba de ser mágica porque aprendías a leer en sus entrañas y podías llegar a comprenderla.

En aquel tiempo un Hacker era aquel que descubría que por mucho que aprendiera sobre sistemas siempre sabía muy poco.

Hacker era el que conseguía programar esa rutina aún más pequeña y bella.

Hacker era aquel que respetaba el trabajo de otros a los que reconocía como iguales.

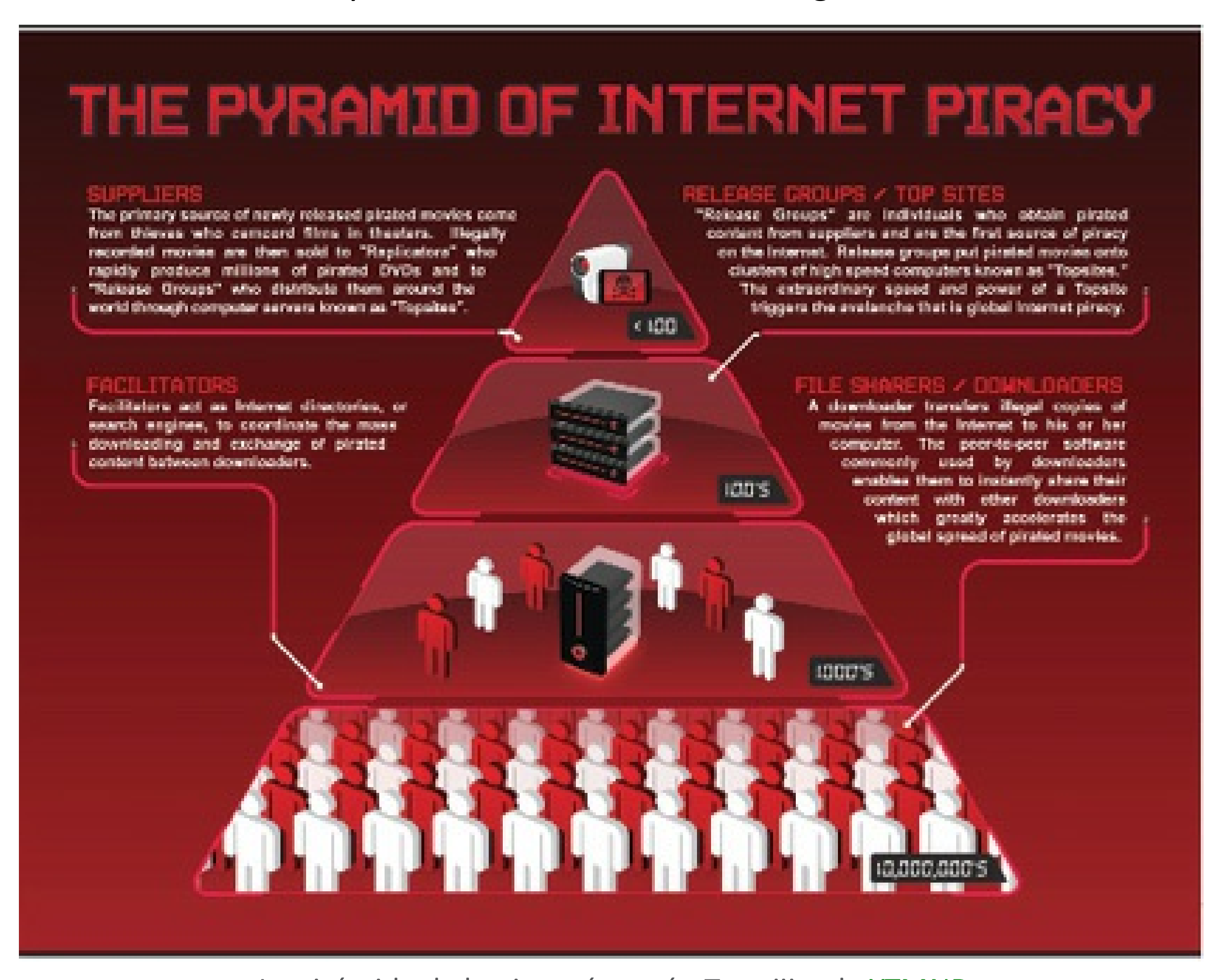
Esta es una página sencilla y un poco espartana, como eran entonces las cosas, dedicada a todos los amigos que tuve la suerte de encontrar por las líneas en aquella etapa, he aquí algunos de ellos :

Ender Wiggins, Omaq, Akira, CenoIx, Agnus Young, D-Orb, Partyman, Quijote/AFL, Pink Pulsar, HorseRide, BlackMan/KhK, Wendigo/Khk, Mave/KhK, El Enano, Bugman, Joker, Spanish Taste, Stoner, binary digitz, Cain, Spectro, GURU JOSH, The Mentor, Savage ...

Que yo recuerde, a ninguno de ellos les he oído o leído nunca llamarse hacker a si mismos.**[2]**

1. La escena warez

La llamada **escena warez** fue la primera de las que componen la *escena hacker*, hasta el extremo de autodenominarse a veces simplemente *la Scene*. Pero en temas tan "underground" los límites son confusos y cabe decir que, a pesar de la confusión popular, la *Scene*, con mayúscula, no es exactamente igual a *escena warez*.



La pirámide de la piratería según Topojijo, de YTMND

Ambas escenas nacieron al mismo tiempo, con la desprotección de juegos y programas. Pero mientras la escena warez distribuía sus productos al gran público y a veces cobraba por ellos, la *Scene*, la élite, eran y son grupos muy discretos de cracking de software distribuido en pequeños círculos, sin ánimo de lucro y en un entorno de competición entre ellos, como bien explican la Wikipedia[3] y la web Scene Group List.

Cabe aclarar también que, en el principio de los tiempos, los programas no se vendían ni compraban. Los hackers que los escribían los regalaban a sus amigos, no existía la noción de intercambiar un programa por dinero. El primer programa que se vendió fue BASIC de Altair, que aseguraba haber escrito Bill Gates, aunque hay serias dudas. Esto molestó mucho a la comunidad hacker, especialmente los que solían reunirse en el primer club de hackers, el Homebrew Computer Club de Silicon Valley.

Uno de ellos, Dan Sokol, alias Nightstalker, escribió un programa que copió el patrón de la tarjeta perforada donde se distribuía el BASIC. Lo pirateó, vamos, y de paso se

convirtió en el primer cracker de la historia. [4]

1.1. Los primeros piratas

El por qué aquellos hackers de los 80 se lanzaron a crackear programas y juegos lo explica muy bien Linus Walleij en su libro “Copyright Does Not Exist”: simplemente, como sus antecesores seguían el viejo axioma de la ética hacker que determina que la información debe ser libre.

> No les gustaba que las compañías de software usasen rutinas de protección de copia que les impedían pegar un vistazo al interior de los programas y copiarlos, para ellos o sus amigos. Querían que aquella información fuese libre.[5]

Y además, claro, estaba el tema económico: no es raro que el phreaking (técnicas para llamar gratis) y el warez fuesen las primeras aficiones de los hackers adolescentes, que les permitían conectarse a las BBS y usar programas de forma gratuita. Además, algunos cobraban por desproteger videojuegos y programas, ingresos que gastaban en comprar material informático.

> Con los ordenadores Atari y Amiga empezó la escena warez y sus cracktros. Guardo con mucho cariño discos de Medway boyz y Pompey pirates en los que metían 2 o 3 juegos con compresores y formateando un disco de 720K por encima de sus posibilidades.[6]



Uno de los primeros anuncios contra la piratería de software en Europa

A finales de los 80 y principios de los 90, *El Rastro* en Madrid y el *Mercat de Sant Antoni* en Barcelona congregaban a decenas de vendedores de juegos y programas pirateados, siendo habituales las redadas[7]. También se compraba warez por correo, a partir de anuncios en revistas especializadas. Cuando llegaron las BBS, se convirtieron en otro canal habitual de difusión de warez junto a otro delito, el carding, la distribución de datos de tarjetas de crédito, robados o creados mediante programas que los generaban, tarjetas de teléfono y otras.

Según la revista “Microhobby”, en 1986 se calculaba que el 80% de programas instalados en ordenadores españoles eran piratas[8]. En diciembre de 1986, la revista publicaba un especial sobre la piratería, donde reproducía una conversación con un vendedor de warez del Rastro:

> -Estas copias como las consigues?
> -Casi todas son traídas de Inglaterra
> -Pero vienen directamente desprotegidas o se desprotegen aquí
> -No, hay gente para desprotegerlas pero esa gente no está en Madrid. Esa gente es de fuera, entoces eso se manda a desproteger… bueno hay gente también aquí en Madrid, es gente antigua que desprotegía y se le sigue mandando esto.
> -Pagáis algo por desproteger?
> -A veces. A veces se paga por desproteger y otras veces se hace por cambio o por otras razones. Hay gente que se gana la vida en el Rastro, otra se la gana desprotegiendo, hay de todos los tipos.[9]

1.2. El Quijote

Prácticamente no hay hacker de aquella época que no hubiese hecho sus pinitos destripando programas y jugando al warez. Destacaron entre otros **El Rocker** y Angeloso, que años después pondría en marcha Isla Tortuga junto con Maki. Una de las primeras páginas de Isla Tortuga fue, precisamente, la dedicada al #canalwarez de IRC-Hispano.

Otro conocido de la escena warez española fue **El Quijote**, un coruñés a quien detuvo la policía. Su historia es peculiar: El Quijote era amigo de Omega, un hacker que trabajaba en la compañía Telefónica de España. Omega realizaba un curiosa labor social consistente en poner una línea gratis en las centrales que montaba, para los hackers que vivían en los edificios cercanos. Omega y El Quijote se conocían de una BBS “underground”, God’s House, y Omega le había puesto una línea gratuita con una condición: sólo debía usarse para transmitir datos, nada de charlas.

El Quijote usaba la línea para descargar warez del extranjero, se bajaba lo que le pedía la gente de la BBS y otros. Pero cometió un error: empezó a hablar por ella y, un día, charlando con uno de sus proveedores de warez, le dio su dirección postal. La policía estaba a la escucha y en poco tiempo los tuvo en su domicilio. Le requisaron cantidades ingentes de disquetes. Cuando le preguntaron por qué tenía una línea gratuita abierta en una central de Coruña, contó la misma película todo el rato: *“Que estaba de copas, un tío le pidió que le invitase y a cambio le dio una línea de teléfono gratis”*[10]. Nunca pudo demostrarse la relación entre Omega y El Quijote.

Otro habitual de la BBS God’s House era Agnus Young, un chaval de 14 años, totalmente antisocial pero a quien le gustaba regalar llamadas de cabinas a las ancianitas.[11]

1.3. SRS & AWD

Depeche Mode era el *nick* del zaragozano Michel Izquierdo. Entró en el mundo del warez en 1983, cuando se compró un Spectrum pero se le averió, dejándole tres meses sin máquina. Gastó ese tiempo leyendo un libro de programación en ensamblador, que aplicó en "sacar las tripas a los juegos que tenía". Entre 1983 y 1986, él y un amigo, Manolo, se dedicaron intensamente a crackear juegos por diversión. Firmaban: *Desprotegido por SRS* (Super Rata Software, uno de los apodos de Manolo) *& AWD* (un indicativo de radioaficionado, de Depeche Mode).

> Formábamos parte de la mayor red de distribución de juegos crackeados de España. Un tío de la universidad de Zaragoza, un coleccionista, nos pasaba una o dos cintas cada semana, con 20/30 juegos para crackear que no sé de dónde sacaba porque le llegaban incluso cosas de Inglaterra. Y se los devolvíamos crackeados.**[12]**

Depeche asegura que no cobraba por los juegos, que pasaba a los amigos, aunque otros sí lo hacían. La actividad crackeadora de la gente de Zaragoza llegó a ser tal que algunas tiendas del Rastro madrileño, que vendían juegos desprotegidos, tenían una sección llamada *Desprotecciones Zaragoza*.

> Víctor Ruiz, de Dinamic, me llamó una vez, que no sé cómo consiguió el número, para que lo dejásemos.**[13]**

Otro grupo de warez de la época lo formaban **Pablo, Santiago y Emilio**. Ellos y *SRS & AWD* protagonizaron la que posiblemente fue primera carrera por una "release" (lanzamiento) en la escena warez española:

> El juego Daley Thompson's Decathlon**[14]** fue el primero que llevaba un sistema anticopia, con un texto que ponía "Desproteger este programa puede ser perjudicial para la salud". Ellos lo desprotegieron primero, nos ganaron por dos horas.**[15]**

SRS & AWD son una firma mítica del primer warez español. Depeche asegura que fueron los primeros que introdujeron efectos, como espirales o líneas, para distraer la espera mientras se cargaba el programa, lo que serían las primeros intros. También crearon grabadores y cargadores de alta velocidad y ponían especial atención en facilitar la copia de los juegos.

> Teníamos una filosofía: nuestras desprotecciones debían poderse copiar con el Copión de Argüello**[16]**, que tenía todo el mundo y que iba bien, además era fácil de escribir y se encontraba en todos los manuales. O se autocopiaban al terminar, con una combinación de teclas.**[17]**

Después del Spectrum, Depeche se compró un Amiga y, más adelante, un PC. En algún momento de este proceso, segunda mitad de los 80, dejó el cracking de juegos de un día para otro. Según cuenta, se cansó. Como otros, había descubierto una nueva afición: el hacking. Entró a trabajar en una empresa donde consiguió un módem de 1.200 baudios, un SmartLink.

2. Glaucoma

Glaucoma es considerado el primer grupo de hackers españoles, en activo entre 1987 y 1989. Lo formaban HorseRide, Han Solo y Depeche Mode, todos de Zaragoza.**[18]**

> “El grupo se llamaba Glaucoma porque atacaban a la red Iris (que conectaba los centros de investigación académica). Desde los ordenadores de la Universidad saltaban a cualquier punto del mundo.**[19]**

En aquella época, un hacker debía saber de todo: phreaking, hacking, warez, programación, hardware... y a ser posible mantener su propia BBS. Depeche y Han Solo montaron una:

> Camelamos a una tienda de informática para que nos dejara un ordenador y una línea, que era compartida y podíamos usar de noche. La BBS se llamó Bauhaus, pero duró poco, 3 o 4 meses, porque a la tienda no le gustó la idea.**[20]**

Más adelante Depeche abriría Scroll Lock BBS, que después cambió su nombre a Public NME (pronunciado *enemy*). Estuvo en activo una década.

2.1. Una joya de 1.200 baudios

Depeche, Horse y Solo se habían conocido a través de la radioafición, puerta de entrada de muchos hackers al mundo de la electrónica y las telecomunicaciones. En 1987 puede decirse que el grupo ya estaba formado y operativo, aunque no tendría nombre prácticamente hasta su disolución.

Depeche había conseguido un módem de 1.200 baudios en la empresa de bases de datos donde trabajaba, lo que en aquellos tiempos era una joya, muy cara y difícil de obtener para un particular, menos aún para un menor de edad. Pero lo complicado no era sólo hacerse con un módem: la factura del teléfono subía hasta la estratosfera al hacer pruebas. Y, además, no era sencillo encontrar otros módems a los que conectarse. En las revistas de electrónica e informática salían listas de BBS, pero no siempre estaban actualizadas.

> Ya tenías el módem, vale, y ahora ¿qué hago?, ¿a dónde llamo? Había listas de teléfonos de BBS pero estaban desactualizadas. Llamé a lo que se suponía eran dos BBS de Zaragoza que no contestaban nunca...**[21]**

Pronto descubrieron un sitio con módems que sí respondían las llamadas: la Universidad de Zaragoza. HorseRide, Han Solo y Depeche Mode se dejaron caer un día por el Centro de Cálculo de la universidad, como si fuesen estudiantes, y pillaron algunos nombres de usuario y contraseñas, usando la técnica del shoulder surfing: espiar por la espalda a quien está tecleando. Ya en casa, llamaron por módem a la universidad y usaron las contraseñas para entrar en sus ordenadores.

2.2. El comando HELP

Cuando conseguían entrar en una máquina, la primera palabra que tecleaban era

HELP, pues con esta instrucción la mayoría de programas mostraban su manual de instrucciones. Después era cuestión de leer e ir probando comandos, mientras estaban conectados remota e ilegalmente. Así aprendían cómo funcionaban los sistemas.

En la Universidad de Zaragoza las computadoras eran marca VAX y, mientras las toqueteaban, descubrieron una extraña instrucción: *set host/x29*, que parecía no servir para nada pero allí estaba, incitando su curiosidad:

> Más adelante sabríamos que era el comando para conectar a redes X25, pero aún estaban montando RedIRIS, la red de las universidades, y no funcionaba aún. También descubrimos dos módems más en la universidad, así que ya teníamos tres canales de acceso para entrar: uno para cada uno.**[22]**

En aquellos tiempos, el principal problema para un hacker eran las comunicaciones: descubrir vías para acceder a los ordenadores y redes. Buena parte de su tiempo se gastaba en buscar y, una vez conseguidas, asegurar estas conexiones. Sus principales tareas eran inventar trucos y aparatos para llamar gratuitamente, como las cajas azules o “blueboxes”; localizar puertas de entrada a las redes que tuviesen buenas conexiones, como podían ser módems de universidades o, mejor, empresas; conseguir listas de usuarios y contraseñas para entrar en los ordenadores, y preservar el mayor tiempo posible las infraestructuras conquistadas.

A ese cometido les ayudaban los propios usuarios, empresas e instituciones, que no tenían mentalidad de seguridad informática: eran muy habituales las contraseñas débiles o sistemas sin contraseña. En la universidad eran frecuentes las credenciales de entrada al estilo: *usuario: decano / contraseña: decano*. Incluso en los bancos, como Kutxa, a cuya máquina de pagos VISA se accedía tecleando *usuario: operador /contraseña: operador*.

Por suerte para tanto banco y empresa desprotegidos, aquellos hackers no tenían mentalidad de criminales. Como mucho crackeaban juegos y programas o, como confiesa uno de los integrantes del grupo que llegó después de Glaucoma, Apòstols, usaban comprobantes, pillados en las papeleras de los cajeros, para conseguir datos de tarjetas de crédito con las que pagarse una cuenta en Compuserve, entonces la mayor BBS y proveedor de acceso de Estados Unidos.

A aquellos hackers les importaba poco si el ordenador donde acababan de entrar pertenecía a un banco o al ejército, no era el contenido lo que les llamaba sino el propio sistema, aprender cómo funcionaba y usarlo para sus cosas, como guardar warez o saltar a otras redes. Las máquinas con sistemas operativos más raros eran retos, algunos de los cuales jamás se consiguieron descifrar y, 20 años después, aquellos hackers aún se acuerdan con la nostalgia del perdedor.

2.3. Set host/x29

Un día, probaron otra vez a teclear *set host/x29* y la máquina, por fin, respondió.

Primero no tenían idea de qué era aquello, pero aprendían rápido: el comando les daba entrada a RedIRIS, la red que unía las universidades españolas, gestionada por Fundesco-Telefónica. RedIRIS ofrecía a las universidades -y a los hackers- acceso a las redes X25 del mundo, antecesoras de Internet.

Fue a raíz de haber descubierto cómo asaltar RedIRIS que, más adelante, el grupo decidió llamarse Glaucoma, una enfermedad que ataca el iris y otras partes del ojo.



VAX4000/600 de finales de los años 80, que formaba parte de REDIris



Ambas fotos son extraídas del ACSI Computer Museum

Excitados por el descubrimiento, Horse, Solo y Depeche pasaron un mes entrando y saliendo de RedIRIS, hasta que una noche, como tantas noches que habían entrado impunemente a través de la Universidad de Zaragoza, alguien les abrió un “phone”, que así se llamaba la función de chat en los Vax: se abría una ventana de diálogo en la pantalla del usuario con quien se deseaba chatear. Al otro lado estaba el administrador del Centro de Cálculo:

> Hablamos y vio que había algo raro, aparte de que todo el mundo usaba el sistema de día y nosotros, de noche, por eso cantó. A los dos o tres días la cuenta dejó de funcionar, pero como habíamos conseguido toda la lista de usuarios, entramos por otra, que también nos cerró.**[23]**

Empezó así una carrera del ratón y el gato: cuando les cerraban una cuenta, los hackers entraban por otras, que el administrador les iba cerrando a medida que descubría que estaban comprometidas. El juego duró dos meses en los que su máxima obsesión era usar RedIRIS para salir a las redes X25 de fuera, investigar qué había allí y asegurarse la conexión para el día siguiente. Llegaron así a donde llevaban todos los caminos “underground” en aquellos tiempos: al chat QSD, de la red francesa Minitel, centro internacional de reunión de los hackers de la época. Allí conocerían a algunos hackers catalanes, como Savage y otros, que más tarde formarían el grupo Apòstols:

> QSD era un chat gay y la primera pregunta que nos hacían al entrar era: “¿Eres hacker o gay?”. A partir de aquí, ibas encontrando a gente, te pasaban otros chat.**[24]**

2.4. La venganza del inglés

Por fin, una noche, vieron que ya no les quedaban más cuentas. Estaban usando su

último cartucho y al día siguiente les desconectarían de su aventura en las redes. Llenos de ira, Solo y Horse tramaron una venganza a la que Depeche no quiso sumarse:

> Dejaron en el Vax un proceso funcionando toda la noche, que mandó mensajes a todas las cuentas, más de una vez, avisando de que había una bomba lógica en el sistema y que se iba a ir todo a la mierda. La gente guardaba sus trabajos de doctorado en el sistema y la noticia corrió como la pólvora. Al día siguiente iban todos corriendo y llorando para que les hicieran una copia de sus datos en el centro de cálculo. Incluso salió la noticia en "El Heraldo de Aragón". Posteriormente, HorseRide les contó una versión con la que acabaron dando las culpas a un pobre cabeza de turco, al que echaron de la universidad.**[25]**

Fue el inicio del fin.

> Se pelearon entre ellos, porque nadie quería ir a la cárcel.**[26]**

Pero, aún medio peleados, antes que nada eran hackers y era absolutamente necesario volver a tener salida a X25. Así que HorseRide y Han Solo, a sus 18 años, echaron mano de la ingeniería social y concertaron una cita con Telefónica: se hicieron pasar por comerciales de una empresa que vendía tiempo compartido y quería comprar cuentas X25. Cuando les hacían una demostración, usaron otra vez la técnica del shoulder surfing y pudieron ver el nombre de usuario y contraseña que les daría acceso a los nodos X25 de Telefónica de España.

> Le pillamos a Telefónica el password global de todos los nodos X25: ORTSAC, que era el apellido del tío que lo había hecho, Castro, puesto al revés. Lo pilló Horseride, líder de los Glaucoma, también conocido como IDLC (inglesito de los cojones). Se hizo pasar por un inglés que venía a vender "time-sharing". Cuando se conectaban, el tío miraba el ID y el password, se lo aprendió de memoria y ya lo tuvimos.**[27]**

Poco tiempo después, Glaucoma se disolvió, en 1989. Depeche Mode se integró en el grupo Apòstols.

2.5. Savage

Meses antes otro hacker, Jordi Murgó, conocido como **The Phreaker**, había conseguido la famosa clave ORTSAC, pero en solitario, usando ingeniería social:

> Año 1987 (tenía un modem de 300bps y un ordenador MSX). En una revista del sector leí que las empresas se conectaban por X25 (IBERPAC) y el tema me interesó. El primer paso fue conseguir los números de acceso a IBERPAC... Hice una llamada a información de la CTNE:
>
> - Hola, soy Fulanito de Tal, del departamento de Informática de XXX, y necesito los números de acceso a la red IBERPAC de toda España, para que nuestros representantes puedan acceder a la nueva aplicación de pedidos.
>
> - Espere un momento que le doy el teléfono del departamento de "Datos".
>
> - Hola, ... el mismo rollo ....
>
> - Sí, por supuesto, ¿a qué fax se lo mando?
>
> - Les dí mi número y puse en marcha una mierda de FAX manual (desguazado de unas

oficinas), de los que no pone la identificación del equipo.

Bueno, ya tengo el teléfono de acceso, ahora un manual, a ver cómo funciona... Fui a las oficinas comerciales de Telefónica, les expliqué que mi primo estaba en EEUU y que me había hablado de X25, que en su ordenador de la universidad tenían. Muy amables, me dieron un montón de panfletos, incluido un mini manual de X28 (PAC de acceso a Iberpac)

Me pongo a probar pero, claro, me faltaban "direcciones" X25 para conectar: *Trashing*. Los contenedores que estaban delante del centro Iberpac de Lleida. En una semana ya tenía listados inacabables de direcciones. Muchas aceptaban sólo cobro revertido, o sea, no necesitaba un usuario/password de acceso a Iberpac.

Estuve unos meses jugando con lo que tenía, conseguí direcciones X25 del exterior, pero se necesitaba usuario/password para acceder a Iberpac internacional.

Llamé al Teléfono del departamento de "Datos":

- Hola, soy Manolo de Datos de Huesca, que he perdido la clave para hacer pruebas X28, ¿la tienes por aquí a mano?

- Sí claro, es N918340405/ORTSAC

Y así pude salir del país, y conocer a Apòstols en los chats exteriores (Minitels franceses, pero con acceso X25 internacional). Su procedimiento para llegar allí había sido muy similar.

La clave de acceso ORTSAC era casi universal :) y duró 2 años. ORTSAC era CASTRO, nombre del responsable que la pidió para hacer las pruebas X28 de toda España.

Cuando se petó, intentamos conseguir la nueva, pero la respuesta era "no, ahora han mandado una distinta a cada provincia".

Entonces, un gran empresa informática pasó a ser nuestro proveedor de claves de acceso, llamando a las 2 de la mañana, cuando sólo había un colgado de guardia o un vigilante:

-Hola, soy Manolo Pérez de Iberpac, se nos ha caído el nodo y necesitamos verificar sus datos de acceso...

La conseguimos 3 veces, la de esta gran empresa :)**[28]**

3. Apòstols

Apòstols es el nombre de un grupo de hackers de Barcelona, Lleida, Zaragoza, Alicante y Tenerife que nació en 1989. Su época de mayor actividad se dio entre 1989 y 1991. Tenía 6 miembros: **El Maestro** (Marcial, fundador), **PetaVax** (Enric, fundador), The Phreaker (Jordi Murgó), Depeche Mode (Michel Izquierdo, que venía de Glaucoma), **Sir Lancelot** y Ender Wiggins (Ramón Martínez), aunque entre ellos se apodaban *el primero*, *el segundo* o *el tercero*, según su orden de entrada en el grupo.

> El Maestro, el primero, lo llamábamos así por la puntería y la suerte que tenía, no he visto un tío que llega delante de un ordenador: username, password y dentro. Que lo haga una vez, vale, pero a la de tres...**[29]**

Una lista de los miembros de Apòstols se conserva en el Internet Archive: Members of Apostols Unix Cult



Portada de la web de Apòstols en 1998

Apòstols se fraguó en un chat de la red francesa Minitel, llamado QSD, que era el centro de reunión de los hackers europeos y muy visitado por los norteamericanos. Allí se conocieron El Maestro, PetaVax, The Phreaker y Depeche Mode, cuando aún estaba en Glaucoma.

> El punto de encuentro era QSD porque las conexiones X25 tenían un límite de conexiones simultáneas y el de QSD era el más grande de todos, nunca comunicaba.**[30]**

También frecuentaban el chat de ALTGER (Altos Computer Systems Munich)**[31]** y, ocasionalmente, los de Lutzeifer, Altos y RMI **[32]**. Accedían a ellos por las redes X25. Allí intercambiaban cuentas, ficheros, direcciones, teléfonos de BBS y módems y, en general, información útil para el hacking. Net Runner, The Knight, Nemesis o Snuggle era algunos de los habituales, con quienes Apòstols tenían estrecha relación.

Sus aficiones como grupo eran el phreaking y el hacking, preferiblemente en las redes X25. De forma individual, algunos como The Phreaker o Depeche Mode habían practicado el warez.

La página web oficial del grupo está en http://www.apostols.org . Existió también

http://linux.apostols.org , que mantenía The Phreaker pero ya no está en línea. Puede consultarse en Internet Archive: Linux.apostols.org

3.1. Blueboxes

Asegurarse la conectividad era prioridad número uno para los hackers de aquella época. Esto llevó a los miembros de Apóstols a dedicarse al phreaking, para tener las llamadas telefónicas gratuitas. Entre sus prácticas destacaba el "phreaking más viejo del mundo": llamar desde el trabajo. Ender Wiggins lo llevó hasta el descaro de usar una línea del lugar donde trabajaba, "Diario 16", la línea de los corresponsales, para su BBS[33] The Light. Además, en sus domicilios tenían entre dos y tres líneas telefónicas: al menos una para el módem, detrás del cual estaba la BBS, y una o dos para hackear.

> Nuestras facturas no bajaban de las 60.000 o 70.000 pesetas. ¡Y eso que llamábamos gratis! Pero al estar con esto todo el día, acababas gastando dinero. Prácticamente lo que cobrábamos en el trabajo servía para pagar el teléfono.[34]



De izquierda a derecha, Ender, The Phreaker y Depeche, en 2013

Uno de sus juegos era montar "party lines" a lo bestia: Ender llamaba a Depeche y este, que tenía dos líneas, llamaba a The Phreaker, después unían físicamente los cables. "Se escuchaba fatal", confiesa Depeche Mode. Otra afición era construir aparatos, los llamados *boxes*, para engañar a la centralita y llamar de forma gratuita. Los había de diferentes colores, rojos, negros, beige, según sus funciones[35]. Los más famosos eran los *blueboxes*, que generaban un tono que engañaba a las centralitas y permitía llamar gratis. De aquí salió el verbo *blueboxear*:

> Significa hacerte pasar por una central. Los teléfonos de tonos marcan, la central se entera de lo que has marcado y selecciona la línea por donde tiene que salir, por un enlace gordo, y

> llega a otra central. Este enlace estaba señalizado dentro de banda con sonido que era audible. Cuando el enlace estaba libre, hacía un pitido de 2.500 hertzios. Cuando cesaba el pitido, el enlace sabía que tenía que esperar marcación. Lo que hacías era establecer una llamada gratuita, a Información por ejemplo, y tal como te respondía la operadora soltabas el tono de 2.500 hertzios. El enlace interpretaba que volvía a estar libre, dejabas de dar los 2.500 y el enlace esperaba marcación. De forma que estabas marcando como si fuese una central llamando a otra, no había tarificación de usuario.**[36]**

Fue gracias a una casualidad como Apòstols descubrió la forma de llamar gratuitamente desde España. Habían hecho todo tipo de pruebas, se habían roto la cabeza y no había manera de conseguirlo, hasta que descubrieron que la razón era una pequeña diferencia entre las redes telefónicas españolas y las de Estados Unidos, que imposibilitaba llamar gratis siguiendo las instrucciones de los manuales norteamericanos:

> Lo descubrimos entre todos, gastando una pasta llamándonos. Fue gracias a que algunas señoras de la zona de Girona, cuando decían "digui" (diga) al descolgar, el tono era tan agudo que llegaba a los 2.500 hertzios y cortaba el enlace. Ahí tuvimos la inspiración: ¡Narices, es socotel! Socotel era el tipo de enlace que señalizaba el dentro de banda. Los americanos señalizaban en 2.600, que lo habíamos probado 20.000 veces y en España no funcionaba.**[37]**

A Depeche Mode se le ponen aún los pelos de punta cuando recuerda lo que podría llamarse "el sonido del vacío telefónico":

> Cuando cortabas con 2.500 se quedaba un eco en la línea... Oías tu respiración y siempre te parecía que había alguien escuchando.**[38]**
>
> El eco seguía cuando hacías la llamada gratuita, por ejemplo a Estados Unidos.**[39]**
>
> Era terrorífico.**[40]**

La única publicación de Apòstols como grupo fue un fanzine, escrito por Ender Wiggins, que es el texto más viejo conservado sobre phreaking en castellano: el Manual del novicio al hack/phreack. Allí puede leerse:

> El único medio abierto a la masa de aprendices al Hacking Phreaking en España es el área Hacking de fidonet. En todo el tiempo que llevo leyendo el área, un año más o menos, el anhelo de todos ha sido la Blue Box. No sé si alguno lo habrá conseguido, ya que pistas se han dado las suficientes. (Se han visto incluso esquemas de osciladores digitales, por los cuales se le hecho una reprimenda tremenda al autor :->).**[41]**

3.2. Las redes X25

La mayor diversión o, como lo llama Ender Wiggins, "vicio" de Apòstols era surcar las redes X25. Buscaban ordenadores conectados a ellas, la mayoría con sistemas operativos UNIX**[42]** y VMS (creado por Digital Equipment Corporation para sus mini-computadoras VAX**[43]**), para entrar en las redes nacionales y, desde allí, salir a las internacionales. Una de sus diversiones era dar la vuelta a la Tierra, dando saltos de un nodo X25 al otro sin pagar por ello, muy al estilo de los viejos phreakers, que gustaban de dar la vuelta al mundo saltando de centralita en centralita, también gratis.



Los tres manuales de VAX sobre X25, gentileza de EnderWiggins

Cuando entraban en una máquina, si esta tenía buenas conexiones creaban una zona de chat para los amigos. O bien montaban un *Packet Assembler and Dissassembler* (PAD)[44], que convertía una sesión de módem en paquetes X25, de forma que se podía saltar de allí a las redes X25, o al revés, llamar gratis por teléfono desde las redes. Eran ordenadores de empresas, entidades financieras, universidades y gobiernos, los únicos que podían pagar este tipo de comunicaciones. Tenían un número limitado de conexiones X25 y lo bueno era encontrar una máquina con muchas. También eran muy atrayentes las que aceptaban cobro revertido.

La forma clásica de descubrir ordenadores con acceso a X25 era hacer que el módem fuese probando números, de forma automatizada. Los hackers creaban sus propios programas para ello, que dejaban funcionando mientras dormían o iban al trabajo. A la vuelta tenían una lista detallada, con incluso el sistema operativo de los ordenadores encontrados. Esta técnica, llamada “escanear”, es una de las más habituales en el hacking. Se usaría más adelante para encontrar números 900 (llamada gratuita) desde los que saltar a Internet[45], ordenadores con determinado tipo de vulnerabilidad, etc.

La red X25 española, propiedad de Telefónica, era IBERPAC. Había diferentes métodos de acceso a ella, como X28 y X32. El más usual era X28, con un módem y un PC.

> X28 era para los humanos. X32 era para los dioses porque estaba reservado para las grandes máquinas. Era una forma barata de tener X25 para equipos de oficinas o cajeros en poblaciones pequeñas, donde poner X25 era prohibitivo. Llamabas al nodo de entrada por un puerto serie sincrono, especial, y usaba paquetes. Adapté un software para entrar así,

> emulando una de esas máquinas, pero no tenía el hardware, que tuve que adaptar también, con unos cables.[46]

Lo usual era llamar a IBERPAC con el módem de casa, hacer Intro y pedía un usuario y contraseña. La gran hazaña de los hackers de la época fue hacerse con la contraseña de acceso a IBERPAC, usando para ello ingeniería social. De IBERPAC saltaban a las redes europeas, donde practicaban la vida social con otros hackers:

> Si querías contactar con gente un poco "underground", o llamabas directamente a BBS americanas o alemanas, o no tenías otra salida. Pero, a través de una llamada local, tenías acceso a X25. Lo único que necesitabas era un login y un password y, a partir de aquí, podías saltar a los chats franceses de la red Minitel. Primero accedías a través de las universidades y, en los chats, conseguías métodos para acceder a cuentas directas de X25. Aprendías a hacer hacking social, a llamar por la noche a operadores pidiéndoles directamente el login y password.[47]

Al estar unidas las redes de Europa y Estados Unidos, en una incipiente Internet, no era raro que las sesiones de hacking se alargasen más allá del océano:

> Los nodos de entrada de X25 americanos estaban mal configurados y, si entrabas por detrás, tenías un módem para conectar a donde quisieras del mundo. Sólo necesitabas la lista de nodos, que era fácil de conseguir: cuando entrabas en una universidad americana, mirabas quién estaba conectado y te salía una lista con el número identificador de la puerta de entrada a la red que había utilizado. Si conectabas con aquel identificador, cuando el usuario no estaba, algunos operadores lo tenían mal montado y haciendo poca cosa, AT OK, ya tenías el módem allí. Circulaban listas con cuentas que todo el mundo conocía, una de ellas era RMS, la de Richard Stallman, en una máquina del MIT, sin password.[48]

La principal puerta de entrada a las redes de Estados Unidos era el sistema MITRE, de un proveedor del ejército norteamericano. MITRE se hizo famoso a raíz del libro "El huevo del cuco", de Cliff Stoll, que narra como hackers del Chaos Computer Club[49] lo usaban para robar secretos empresariales de Estados Unidos y venderlos al KGB:

> MITRE estaba muy bien comunicado con todas las redes activas entonces. Había un menú de entrada para acceder a un servicio de directorio de teléfonos, que podías abortar apretando una secuencia: CTRL-Y **Interrupt**. Si lo hacías bien, abortabas el menú, salías a una shell y desde allí podías conectar a cualquier sitio. Era conocido por casi todo el mundo y, durante años, todos los hackers entraban por allí.[50]

3.3. Hacking

Apòstols gustaban de entrar en ordenadores ajenos por dos razones básicas: diversión y ansias de conocimiento. Importaba poco que la máquina perteneciese al ejército norteamericano o a un banco, lo que ellos buscaban era poder manejarla. Así, hackeando los ordenadores y curioseando en ellos, horas y más horas por las noches, aprendieron los sistemas operativos VMS (para los VAX) y UNIX, a programar en C: y otros lenguajes, etc. Cuánto más rara o exclusiva fuese la máquina, más grande era el reto.

> Lo que buscábamos era tocar sistemas que no estaban a nuestro alcance. Lo primero que hacías cuando entrabas en uno era teclear HELP, era el comando que más usábamos.[51]

Ender Wiggins tiene una graciosa anécdota respecto a esta particular forma de aprendizaje:

> Conseguí trabajo en “Diario 16”, demostrándoles que sabía manejar el sistema operativo de VAX, VMS. Pero cuando llegué el primer día no sabía dónde tenía el interruptor, ya que no había visto un VAX en mi vida, sólo había entrado en ellos.**[52]**



HP9000 con un sistema operativo HP-UX 6.X. El fichero /etc/password de este Unix contenía la clave cifrada de cada usuario y era fácil saber qué usuarios no tenían, buscando los campos “clave” en blanco. ACSI Computer Museum

En los años 80, la seguridad informática era una gran desconocida y aquellos hackers podían campar a sus anchas, en algunos sitios más que en otros, como la Universitat de les Illes Balears, donde habían conseguido la contraseña del rector y podían leer su correo electrónico. Una noche, a las 3 de la mañana, se “aparecieron” al operador de un sistema mediante la utilidad “Phone” de VMS, que como el “Talk” de Unix abre una ventana de chat en la pantalla. Y en ella el atribulado operador puedo leer: *Ave María hermano, los Apóstols están contigo*.**[53]**

Se rieron tanto con la broma que la usaron otras veces, como frase estándar, en otros sistemas, pero no muchos ya que lo mejor era pasar desapercibidos, para que no les descubriesen y poder seguir aprendiendo o experimentando con la máquina.

> Si entrábamos en un Unix, teníamos una perfecta imitación del login que nos permitía utilizar cualquier cuenta del sistema con el password “joshua!” (¿podríamos decir que ya era un rootkit? :) En los VAXes, no podíamos sustituir el LOGIN.EXE, así que hacíamos usuarios que pareciesen procesos del sistema (SYS$PROCESS, por ejemplo) pero con privilegios.**[54]**

Sólo manipulaban del ordenador lo necesario para poder volver a entrar otra noche y, aparte de esto, no modificaban ni rompían nada. Los daños colaterales de sus acciones los padecían Telefónica, cuando hacían phreaking para llamar gratis, y las empresas y organismos propietarios de las conexiones X25, que pagaban sin saberlo las excursiones de Apòstols por las redes.

Nunca les pillaron pero, si les hubiesen pillado, poco habría pasado: ni el phreaking ni el hacking eran delito entonces (el hacking no lo sería hasta el año 2010). Cuando pillaban a alguien haciendo phreaking normalmente era porque había usado el par piloto[55] de su edificio para hacer llamadas[56]. Según la leyenda, el primer condenado por esta causa en España fue HorseRide, el líder de Glaucoma, a quien detuvo la Guardia Civil en 1992. Pero no por llamar gratis, ya que no era delito, sino por robo de fluido eléctrico. Tuvo que pagar una multa.

Otro que acabó detenido, aunque no está claro si también condenado, fue Petavax, de Apòstols, pero tampoco por hacking o phreaking sino por un delito contra la propiedad intelectual:

> Una noche, en casa de Petavax, estuvimos toda la noche haciendo hacking, entramos en la Universitat Politècnica de Catalunya, nos paseamos por todas partes. No habíamos dormido y, por la mañana, a primera hora, llamaron a la puerta. Eran tres señores, uno venía a levantar acta y dos eran de la policía judicial. La noche anterior habíamos tenido un pequeño acojone porque se nos había quedado una llamada enganchada y no se soltaba, nos cogió la paranoia, enchufamos 220 a la línea de teléfono para hacerla saltar y saltó. Pero claro. Cuando a las 9 de la mañana alguien llama a la puerta… nos cagamos.
> -¿Y?
> -Al final, no tenía nada que ver. Se llevaron el ordenador, con todos los logs de la sesión de la noche, todo, los disquetes, y fue porque el compañero había anunciado en una revista que intercambiaba o vendía programas de PC y le había vendido un dBase III a uno de la judicial. El chaval no ha vuelto a ver el PC.[57]

3.4. BBS propias

Además de rondar por las redes X25, charlar con otros hackers, entrar en ordenadores y aprender UNIX, la mayoría de Apòstols tenían su propia BBS, donde ofrecían espacio a la comunidad para hablar en los foros de la BBS o intercambiar textos, programas y juegos, amén de impulsar la conexión de Fidonet, la red que unía a la mayoría de BBS, a Internet. “Toda BBS que se preciase tenía que tener el Libro de Cocina del Anarquista, el *Anarchist Cookbook*”[58], recuerdan riendo los Apòstols.

Sir Lancelot mantenía la BBS ACTIVE SENSE, en Tenerife. Depeche Mode, desde Zaragoza, montó SCROLL LOCK BBS, que al cabo de un año pasó a llamarse PUBLIC NME BBS y así se mantuvo una década, siendo uno de los principales nodos del warez en España.

Ender Wiggins, conocido también como **Captain Fluke** y **Rampa**, abrió ENCOMIX BBS en Monóvar (Alicante), en 1987, que en 1992 se convertiría en uno de los primeros proveedores de Internet (ISP) españoles[59][60][61], al ofrecer correo

electrónico y acceso a newsgroups, primero a través de Fidonet y después, de Internet. Más adelante, Ender abrió THE LIGHT BBS, donde puso todos los textos que había acumulado sobre hacking y phreaking. Algunos pueden verse en el vídeo que realizó uno de sus usuarios, Antonio Martín, alias *Partyman*. Pero conectar la BBS a Fidonet trajo algunos problemas para Ender Wiggins:

> La gente de Fidonet no quería que hubiese estos temas en la red y tenía denuncias cada día. En Fidonet sólo se podía hablar de hacking o de virus, pero no publicar código.**[62]**

ThePhreaker, también conocido como **Savage**, montó su BBS, MSX-ACC (Associació Catalunya Cracker), en 1987 en Lleida, con un módem de botones de 300 bps. Allí intercambiaba juegos y programas para MSX. Los pasaba de cartucho a cinta para que pudieran ser copiados. En 1989, en una segunda línea, montó otra BBS, SAVAGE SOFTWARE, para los amigos. En 1993 puso en marcha el proveedor Lleida.Net Serveis Telemátics.

El tráfico en sus BBS era tan grande que a Ender Wiggins Telefónica le amenazó con denunciarlo por creer que tenía montado un locutorio. A Depeche Mode cada año le visitaba un comercial para que contratase una nueva línea, dada la enorme cantidad de gente que llamaba a su BBS.

> La BBS siempre comunicaba y la gente ponía el módem en autodial para que fuese intentando la conexión, con lo que tenía un montón de intentos.**[63]**

3.5. Modo pausa

Apòstols abandonó su actividad de hacking en 1991, cuando aparecieron Internet y los sistemas libres Linux y FreeBSD, por lo que ya no era necesario asaltar un Unix para usar este sistema operativo. También se complicó el usar *blueboxes* para llamar gratis porque, en 1992, Telefónica de España digitalizó su red nacional y quedaban registrados el origen y destino de las llamadas, haciendo más fácil la persecución de los phreakers. Además, las puertas de acceso a redes X25 se fueron cerrando porque las empresas ya tenían Internet, o "quemando" al ser conocidas por cada vez más gente, o bien porque sus propietarios recibían grandes facturas provocadas por el uso que les daban los hackers, y decidían mejorar su seguridad.

Depeche Mode montó una franquicia de videojuegos, mientras Ender Wiggins y The Phreaker se enfrascaban en convertir sus BBS en proveedores de acceso a Internet. El resto de Apòstols se fueron distanciando.

El grupo vivió una segunda época en 1996, de la mano de The Phreaker, entonces más conocido como Savage, y Ender Wiggins, entonces conocido como Rampa. Por primera vez el grupo tuvo dominio y página web: http://www.apostols.org.

Savage y Rampa se re-unieron, después de haber creado sus respectivos ISPs, Lleida.Net y Encomix, para crear la que sería más importante red de chats que ha existido en España: IRC-Hispano, en 1996. Rampa ayudó también a Savage cuando este se unió a los hackers portugueses ToXyN para montar una de las primeras campañas hacktivistas de la historia de Internet, contra el gobierno de Indonesia y

a favor del Timor Oriental. Savage colaboró bombardeando y asaltando sistemas gubernamentales y haciendo exploits a medida para atacar los sistemas del gobierno.

Posteriormente, Apòstols desapareció de la esfera pública, aunque no se ha dado nunca por muerto de forma oficial. En su página web, aún en activo, se entiende que sigue existiendo como grupo:

Integrist Unix Cult**[64]**

4. Ingeniería social

Junto al phreaking, la ingeniería social era una valiosa herramienta para aquellos primeros hackers a la hora de conseguir información. Uno de los mayores expertos en ingeniería social fue el gallego LeStEr ThE TeAcHeR, quien escribió un conocido Curso de ingeniería social, del que a continuación reproducimos algunas partes.



4.1. Qué es Ingeniería Social

El conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

Puede ser ingeniería social el obtener de un profesor las preguntas de un examen o la clave de acceso de la caja fuerte del Banco de España. Sin embargo, el origen del término tiene que ver con las actividades de obtención de información de tipo técnico utilizadas por hackers. En muchos casos los ingenieros sociales no tocan un ordenador ni acceden a sistemas, pero sin su colaboración otros no tendrían la posibilidad de hacerlo.

En el mundo de las empresas de alta tecnología en las que se desarrollan proyectos reservados, donde la calificación técnica necesaria para entender la información que se quiere obtener es muy alta, las operaciones de ingeniería social de este nivel pueden llevar meses de cuidada planificación y de evaluación de muchos parámetros, yendo más allá de una actuación puntual basada en una llamada con más o menos gracia o picardía.

Otras veces, el ingeniero social simplemente observa el entorno y aprovecha datos que están a la vista. Es el caso de un servidor de la Agencia Tributaria española cuya contraseña está puesta en un "post-it" en su pantalla.[65]

4.2. Primero, el phreaking

Lo que uno podía encontrar en una BBS de aquella época eran ficheros agrupados por temas y mensajes que corrían de unos usuarios a otros, utilizando la base de lo que después sería la red Fidonet u otras basadas en la misma tecnología.

En estas redes, las llamadas entre los nodos las realizaban usuarios "mecenas" que

corrían con el precio de esas llamadas. Los módems eran muy lentos, 1200 o 2400 bps. los más rápidos, y las llamadas eran muy caras. Esto tenía como consecuencia que un usuario no pudiera bajarse toda la información que quería ni conectarse a demasiadas BBS, so pena de arruinarse con la factura del teléfono... o arruinar a sus padres.

Así las cosas, era difícil compartir información propia con otros usuarios y más aún conseguir información técnica interesante que sí se podía encontrar en otros lugares de Europa y Estados Unidos. Los grupos de hackers buscaban formas de abaratar las llamadas de teléfono y conectarse a otros lugares. En su mayoría menores con edades entre los 11 y los 20 años, no disponían de más ingresos que la paga del domingo.

El phreaking era casi una necesidad y había en nuestro país verdaderos magos del sistema telefónico que proveían de "soluciones" para que los demás pudieran pasar el mayor tiempo posible conectados con el menor coste. Es importante entender que si un usuario español deseaba una información de una BBS finlandesa, debía llamar a Finlandia y conectarse a dicha BBS, ya que no había redes que compartieran la información de las BBS del Underground.

En muchos casos, para conseguir informaciones de cómo utilizar ciertas funcionalidades de una central de telefónica, o el acceso a una red, era necesario el uso de ingeniería social. Así, algunos hackers comenzaron a especializarse en esas tareas. El abanico de posibilidades se multiplicó: no sólo el sistema telefónico sinó las configuraciones de servidores, contraseñas de sistemas, datos de compañías empezaron a ser objetivo de los ingenieros sociales, que al facilitárselos a otros hackers les facilitaban en mucho sus tareas, ya que se podían dedicar a lo que realmente les interesaba, aprender sistemas.

Son los tiempos en los que nacen !Hispahack, Apòstols, AFL, KhK Conspiradores y muchos otros grupos ya extinguidos. En cada uno de ellos hay por lo menos un experto en ingeniería social, o bien buscan a especialistas en esta materia para temas concretos.

Se produce un fenómeno interesante a este respecto: la práctica de técnicas de ingeniería social para conseguir información de otros grupos de hackers.**[66]**

4.3. Algunos ingenieros sociales españoles

LeStEr les conoció en la BBS God's House y escribió una aventura de cada uno, que reproduce en su Curso de ingeniería social. Pueden leerse también en Hackstory.net: Agnus Young, D-Orb, LeStEr ThE TeAcHeR, Omega. Por falta de espacio, reproducimos sólo una operación de ingeniería social, protagonizada por The Saint, que mezcla la técnica del *trashing* (mirar en la basura), el uso del teléfono y, lo más delicado en ingeniería social: la visita presencial.

> Como otros muchos, utilizaba un acceso intermedio en un sistema local para poder conectarse a Internet, ya que cuando esto sucede no había proveedores en nuestro país.

Durante mucho tiempo utilizó el mismo acceso, pero ahora sabía que los datos para el acceso al sistema local se cambiaban a primeros de mes. Sabía también que las claves llegaban por carta al apartado de correos que el CPD de aquella caja de ahorros tenia en una ciudad de Aragón. Lo había sabido porque al lado de su instituto tomaban todos los días café algunos directivos de la compañía y a él le gustaba ir allí a "estudiar". Tardó mas o menos un par de meses en enterarse de ello ya que estos directivos siempre se sentaban en la misma mesa y era sencillo escuchar lo que decían.

Conocía varios datos más acerca de la compañía porque cuando las limpiadoras sacaban las bolsas de basura él buscaba entre los papeles listados de las aplicaciones en Cobol o trabajos del Host IBM que tenían allí, un 3090 Sierra. Se acercaba final de mes y necesitaba conseguir la llave de aquel apartado de correos y así poder conseguir las claves de acceso por X.28.

Buscó en la guía el teléfono de la oficina de correos cercana a aquellos edificios y preguntó por el responsable de los apartados. Utilizó un micrófono preamplificado y un altavoz que realzaba los graves para hablar, curiosamente de un órgano electrónico muy barato que hacia sampling .

- Buenos días, Emiliano Pérez al habla dígame que desea?

-Hola, me llamo Federico Tomas de la "caja grande y azul" tenemos ahí un apartado de correos al que va a llegarnos una carta urgente y la llave la tengo en mi poder aquí en Paris. He tenido que venir en viaje de trabajo y no vuelvo hasta dentro una semana. Si le parece bien mandaré a un mensajero para retirar la copia y así poder revisar el correo que es muy urgente.

- No se preocupe, que venga que yo le espero hasta las 2, dígale que venga de su parte para que no haya confusión.

No pasaron más allá de 30 minutos cuando The Saint con un casco de moto y una cazadora de cuero (ambas cosas prestadas) entraba en aquella pequeña oficina de correos y preguntaba por don Emiliano de parte de Don Federico.

- Hola, venía porque mi jefe se ha marchado con la llave del apartado de correos de la empresa y me han dicho que tenía que darme una copia o no sé qué.

- Sí, precisamente aquí la tengo preparada.

- Pues muchas gracias por todo, vuelvo corriendo a la oficina.

- De nada chaval, hasta otra.

Cada vez que llegaba una nueva contraseña The Saint la obtenía y la depositaba de nuevo en aquel apartado de correos solo unas horas después.

A partir de ese momento y durante varios meses The Saint estuvo entrando por una conexión X.28 a aquel banco y desde él y gracias a las contraseñas que recibía cada mes saltaba a otros servidores de la red X.25 que le permitían la salida fuera del país. No hubo denuncia alguna, nadie se enteró nunca y sólo dejó aquellas entradas cuando cambió de ciudad. The Saint trabaja ahora en una importante compañía de seguridad fuera de nuestro país.**[67]**

5. Notas

1. ↑ Código Hispano. Mercè Molist (13/02/01)
2. ↑ LeStEr ThE TeAcHeR
3. ↑ Scene. Es.Wikipedia
4. ↑ Subculture of the subcultures. Linus Walleij. “Copyright Does Not Exist” (1998)
5. ↑ Subculture of the subcultures. Linus Walleij. “Copyright Does Not Exist” (1998)
6. ↑ Anuncio antipiratería de los 80’s . Comentario de musg0. Menéame (09-08-09)
7. ↑ Duro golpe a la piratería. “Microhobby” (15/21-10-85)
8. ↑ Pacto “AFYVE”-”ANEXO” contra la piratería. “Microhobby” (1986)
9. ↑ El punto de vista de los piratas del Rastro. Especial *La piratería*. “Microhoby” (12-86)
10. ↑ Lester, en conversación privada
11. ↑ Lester, en conversación privada
12. ↑ Depeche Mode, en conversación privada
13. ↑ Depeche Mode, en conversación privada
14. ↑ Daley Thompson’s Decathlon. Videojuegos Olvidados. Poetamaldito.com
15. ↑ Depeche Mode, en conversación privada
16. ↑ Copinones. Es.comp.sistemas.sinclair
17. ↑ Depeche Mode, en conversación privada
18. ↑ Comentario #16. La historia de !Hispahack, los primeros hackers españoles. Menéame (16/01/08)
19. ↑ Asalto a La Moncloa. Ildefonso Olmedo “El Mundo” (15-08-99)
20. ↑ Depeche Mode, en conversación privada
21. ↑ Depeche Mode, en conversación privada
22. ↑ Depeche Moden, en conversación privada
23. ↑ Depeche Mode, en conversación privada
24. ↑ El tercer hombre. @rroba, 95 (04-05)
25. ↑ Depeche Mode, en conversación privada
26. ↑ El último apòstol. Mercè Molist. @rroba, 130 (07/08).
27. ↑ El último apòstol. @rroba, 130 (07/08).
28. ↑ Jordi Murgó, en conversación privada
29. ↑ Ramón Martínez: El último apóstol. *Mercè Molist para “@rroba” (28-05-08)*
30. ↑ El tercer hombre. @rroba, 95 (04-05)
31. ↑ Chats. The Hacker Chronicles II.
32. ↑ Renegade Legion Technical Report 1.0: TRW Information
33. ↑ BBS. Es.Wikipedia
34. ↑ The Phreaker, en conversación privada
35. ↑ Descripcion de las cajas de colores. Case Zer0. Iberhack
36. ↑ El último apòstol. @rroba, 130 (07/08)
37. ↑ El último apòstol. @rroba, 130 (07/08)
38. ↑ Depeche Mode, en conversación privada
39. ↑ The Phreaker, en conversación privada
40. ↑ Ender Wiggins, en conversación privada
41. ↑ Manual del novicio al hack/phreack. Culturahack
42. ↑ Unix. Es.Wikipedia
43. ↑ VAX. Es.Wikipedia
44. ↑ PAD. En.Wikipedia
45. ↑ Líneas 900 (1998)
46. ↑ The Phreaker, en conversación privada
47. ↑ El tercer hombre. @rroba, 95 (04-05)
48. ↑ El tercer hombre. @rroba, 95 (04-05)
49. ↑ Chaos Computer Club

50. ↑ El tercer hombre. @rroba, 95 (04-05)
51. ↑ Depeche Mode, en conversación privada
52. ↑ Ender Wiggins, en conversación privada
53. ↑ El último apòstol. @rroba, 130 (07/08)
54. ↑ El tercer hombre. @rroba, 95 (04-05)
55. ↑ Qué es el par piloto. Santiago Fernández. EMTT (29-10-08)
56. ↑ Absuelto un acusado de estafar casi veinte millones a Telefónica. Mercè Molist para "Ciberpais" (1998)
57. ↑ Savage: El tercer hombre. Mercè Molist para la revista "@rroba" (23-05-05)
58. ↑ The Anarchist Cookbook. En.Wikipedia
59. ↑ EncomIX, by Ramón Martinez. Historia de Internet en Aragón. Rampa 1995
60. ↑ Historia de la creación, El Genesis. Encomix (12-03-09)
61. ↑ Mapa de las lineas de EncomIX en 1997. Encomix (05-08-08)
62. ↑ Ender Wiggins, en conversación privada
63. ↑ Depeche Mode, en conversación privada
64. ↑ Página web de Apòstols
65. ↑ Ingeniería Social 1.0. LeStEr ThE TeAcHeR
66. ↑ Ingeniería Social 1.0. LeStEr ThE TeAcHeR
67. ↑ Ingeniería Social 1.0. LeStEr ThE TeAcHeR.

6. Enlaces externos

6.1. Escena warez

· Don't copy that floppy! (1992)
· Warez. Es.Wikipedia.
· La "scene" nacional en el mundo DivX. Enrique Rivas. Diariored (2002)
· Demoscene española
· Warez Scene. En.Wikipedia.
· The History Of The Warez Scene (unfinished). Ipggi & Defacto 2 (1998).
· The Recollection Magazine. Recollections of the early scene.
· C64 Scene Mag Archive
· The Pyramid of Internet Piracy

6.2. Glaucoma

· Historia de Internet en Aragón. Rampa 1995.

6.3. Apòstols

· Presentación de Apòstols en la RootedCon 2010.
· IBM spanish blue box, by Fluke (Fluke era el apodo de EnderWiggins antes de entrar en Apòstols).
· Manual del novicio al hack/phreack. EnderWiggins. Culturahack
· Web de Apòstols en Archive.org
· Aprende el funcionamiento de la Beige Box. TDD.
· Cómo pincharle la línea a alguien.

6.4. Ingeniería social

· Ingeniería Social. Adrián Ramírez.
· Ingeniería Social: Mentiras en la red. Mercè Molist.
· Ingeniería social (Seguridad informática). Wikipedia.
· social engineering. Jargon File.

CAPÍTULO TRES

H/P/A/V/C

H/P/A/V/C

En los años 90, los conceptos *lado oscuro* y *underground* se unen como pegamento a la imagen del hacker. Por una parte debido a la influencia de los medios de comunicación y las fuerzas de la ley, que transmiten el estereotipo del oscuro criminal informático. Por otra parte, la nueva comunidad hacker, la tercera generación, se siente cómoda con la imagen del pirata, el *salteador de la red*. Así, la palabra hacking abandona su significado más generalista, como acción de un hacker, para ceñirse sólo a entrar ilegalmente en un ordenador.

Por unos años se olvidará que, según la definición primigenia, hacker es quien sabe mucho de redes, o quien *"escribe código de forma entusiasta"***[1]**. Los recién llegados, adolescentes en su mayoría, verán más divertido el juego del destructor, del hacker como "revienta máquinas", en un mundo donde este juego es fácil porque la seguridad informática brilla por su ausencia. No será hasta más adelante, con el auge del software libre, cuando se recuperará el arquetipo del hacker como creador de redes y programas.

Cabe aclarar que, aunque la segunda generación también "reventaba" sistemas, esta práctica no era un objetivo en sí mismo, como sí lo será para los hackers de los 90. Glaucoma y Apòstols usaban técnicas de ingeniería social o fallos en programas para saltarse las escasas barreras que encontraban en redes y ordenadores, pero normalmente como paso intermedio hacia el verdadero objetivo: aprender el funcionamiento de esas redes y servidores.

Ahora bien, aunque la ilusión de la tercera generación sea entrar en los sistemas, por el simple reto y mérito, la razón que empuja a esos chavales sigue siendo la que empujó a sus hermanos mayores: la curiosidad, las ganas de aprender, de innovar. Sólo cambia el escenario: si ya ha habido quien ha hecho las máquinas, quien ha escrito los programas y quien ha montado las redes, ¿qué le queda por hacer a esta nueva hornada? Pues jugar a poner el invento patas arriba, buscando sus fallos y límites, aprendiendo casi sin darse cuenta la relevante -y en el futuro imprescindible tarea- de hacer seguras las redes.

La tercera generación es hija legítima de la segunda, que en ocasiones le hace de maestra. Ejemplo primero es la difusión del Manual del novicio al hack/phreack, obra de Ender Wiggins como legado de Apòstols a los que les siguieron. En las BBS, en el IRC, en los grupos de noticias, en el área Hack de Fidonet, veteranos enseñan a los novatos, que cada vez son más.

A veces de la mano de los maestros, a veces de los propios novatos llenos de curiosidad, surgen los primeros textos en castellano sobre hacking, muchas traducciones, recopilaciones de enlaces, nacen multitud de ezines, aunque pocas sobrevivirán más allá del segundo o tercer número: Virtual Zone Magazine, SET, Cyberhack, Webhack, The Young Hackers of Spain o Hack Navigator. Aunque esta última sólo sacó un número, su *staff* concentra algunos de los nicks clave de la

escena hacker española de aquellos años: Warezzman (de Iberhack, CPNE, SET...), Homs, Guybrush (de Raregazz)...

Curiosamente, la mayoría de nombres clave de la escena hacker procede del Levante español. No está claro el por qué, pero así es: Catalunya, Castelló, València, Alicante, Murcia, Almería, parte de Andalucía y parte de Aragón son la cuna de buena parte de hackers de los 80-90, siendo Murcia la zona con más hackers por metro cuadrado. *Los pretorianos* es un grupo ejemplar en este aspecto, pues sus muchos miembros (Belica, Alttab, Ipas, Tdp, Markitos, Fragel, AcidKrs, Ufo, Cyborg, _X_, Danko, Opalo, etc) cubrían todo el arco mediterráneo: Valencia, Alicante, Murcia, Almeria, Granada, Málaga...

La mayoría de grupos o bandas de hackers de principios de los 90 nacen en las BBS, bien porque se conocen en reuniones de usuarios de la misma, bien porque brillan por sus mérito y se les invita a la zona oculta o élite de la BBS.

> El reunirse en grupos supone un importante cambio sociológico pues los hackers son, en su mayoría, autodidactas que han aprendido muchísimo en la soledad de su habitación, leyendo manuales, conectándose a lugares de los que aprendían; sin embargo, es cuando comienzan a trabajar en equipo cuando sus logros se hacen más importantes y, aunque existe el celo por la información, dentro del grupo esta se comparte de una manera fluida.**[2]**

Auténticas canteras de hackers, muchas BBS tenían un rincón cuyo contenido se presentaba con una retahíla de letras: **H/P/A/V/C**, a veces menos (H/P/V/C o H/P). Significan **Hacking/Phreaking/Anarchy/Virii/Cracking**, aunque a veces la *C* se refiere a carding. Son las artes del hacker de los 80-90, su caja de herramientas: el hacking para asaltar servidores ajenos, el phreaking para no pagar el teléfono, los virus para programar intrusos, el cracking para des-programarlo todo, y la anarquía como moral.

A partir de los 90, habrá BBS que ya no dedicarán un rincón al hacking sino que se dedicarán exclusivamente a estos temas. Es por ejemplo la BBS The Light, de Rampa, Public NME, God's House, Jurassic Park, Dark Node, VampireBBS o Waikiki Island. Sitios de acceso restringido donde sólo podían entrar personas de confianza del administrador.

Pero, al mismo tiempo que el hacker crea zonas ocultas en las BBS o canales de chat privados, se preocupa también por expandir la información que según su criterio puede ser publicitada, especialmente aquella que facilita el aprendizaje. Así, en la primera mitad de los 90 se abren los primeros canales de IRC donde la comunidad hacker puede hablar en castellano. En Undernet surgen #warezspain, #esphack o #!hispahack, que en 1993 dará lugar al grupo !Hispahack.

Los grupos de hackers son aún poco a principios de los 90 y sus integrantes pueden considerarse aún pioneros de la segunda generación. Algunos destacan por su singularidad, como los Dalton, el primer grupo conocido de escritores de virus en España, activos entre 1990 y 1991. Son cuatro, entre ellos Jordi Mas, quien años después liderará el proyecto de traducción de programas Softcatalà.

Los Dalton escriben virus de 16 bits. Su creación más conocida es *Anti-Tel*[3], uno de los primeros virus que se transmite vía disquete y se copia al disco duro, donde queda residente hasta que, pasado un tiempo, lanza el mensaje: **Telefónica siempre jodiendo** y borra la FAT del ordenador.

Los Dalton crearon también un primitivo antivirus, *Skudo*, que observaba si había operaciones malignas en el sistema. Después de mucho trabajo y pruebas, consiguieron que Skudo no detectase al virus Anti-Tel... y entonces y sólo entonces lo lanzaron al ruedo, a infectar disquetes.



Web de -S.H.E.- con el típico fondo oscuro con estrellas, estilo *Star Wars*

En 1993 aparecen más grupos: los madrileños Konspiradores Hacker Klub, con Mave y el gallego Lester; Big Bro Killerz, con Tosh y Rek2WiLdS, grandes traductores de textos como Hackers con causa; el Sindicato de Hackers Españoles, con Wendigo, Trader, Raider y FutureMan, o Legion Oscura con Galahad, activo al menos desde 1996 según Internet Archive.

La World Wide Web, el último gran invento de la primera generación de hackers -junto con el software libre-, empieza a popularizarse en 1992. En septiembre de 1993, Jordi Adell, Toni Bellver, Carles Bellver, Enrique Navarro y Enrique Silvestre, de la Universitat de Castelló, montan el primer servidor web de España.

Como ha sido siempre, los hackers lo inventan y los hackers lo usan antes que nadie: las primeras páginas en la web con información sobre hacking son básicamente directorios de enlaces a webs norteamericanas, en las páginas personales que las universidades permiten tener a sus becarios e investigadores. En 1994 aparece Geocities, el primer servicio que ofrece espacio web gratuito. Allí se construyen las primeras casas de los grupos hackers, como BBK, -S.H.E.- y Legion Oscura. Todas con el obligado fondo negro, recordando la estética de la consola.



Web de Iberhack, con el fondo gris de las primeras páginas de la World Wide Web

El problema vendrá cuando algún alma, cándida o demoníaca, informe al servicio de alojamiento que en aquella página hay contenidos de hacking, lo que significa cierre inmediato.

Por un chivatazo tal que así morirán los sitios en Geocities de BBK, La Vieja Guardia, SET o el veterano sitio de información Iberhack, nodo central desde 1996 de todo lo interesante en la web sobre hacking en castellano. El refugio de muchos será Isla Tortuga, una especie de Geocities sólo para gente del H/P/A/V/C -y si había P (de porno), mejor- hispano. Isla Tortuga nació en 1996 y, con ella, la muestra pública de que existía una escena hacker, que allí tenía su escaparate.

La puesta en marcha de Infovía, en 1995, hace surgir multitud de proveedores de acceso a Internet, lo que abarata precios. Además permite conectarse desde prácticamente cualquier pueblo y no sólo las capitales. Todo esto provocará un *boom* de nuevos usuarios, que se reflejará también en la comunidad hacker, donde aparecen multitud de nuevos grupos.

Ante esta sobrepoblación, el hacker renacentista de principios de los 90, con su navaja suiza H/P/A/V/C de conocimientos que controla en su conjunto, pasa a ser un hacker especializado que ahonda sólo en una de las artes: aparecerán grupos de *phreaking* o de *cracking*, aunque serán los menos, pues la mayoría se dedicarán al *hacking*, entendido para siempre como asaltar la seguridad de sistemas informáticos. Otra cambio, a mediados de los 90 y gracias a Infovía, es que el chat sustituye a las BBS como sitio de reunión habitual de la comunidad hacker y lugar de nacimiento de los grupos.

A partir de 1994, muchas BBS se reconvierten en ISPs: EncomIX, Arrakis, LleidaNet, Servicom, Minorisa, Cinet69, ASERTEL, Abaforum, Intercom. En 1995, Infovía y una agresiva política de Telefónica hicieron multiplicar exponencialmente los ISPs, permitiendo que incluso empresas no tecnológicas, como los bancos, regalasen acceso a Internet. Esto dio lugar a anécdotas como la que recuerda Josu Aramberri,

profesor de la Universidad del País Vasco-Euskal Herriko Unibertsitatea, donde un joven hackeaba usando el acceso a Internet que el banco regalaba a su padre:

> Un alumno se dedicaba a entrar en las máquinas de la universidad, mediante la cuenta de acceso gratuito que sus padres tenían en una entidad financiera. Siempre borraba las trazas de sus fechorías, hasta que un día logramos rastrearlas. Pero no había manera de descubrir quien era. Al llamar al banco que actuaba como proveedor de internet quejándonos, dieron de baja ese usuario. Y recibimos una indignada llamada de los padres, descubriendo sin saberlo a su hijo... Los sucesos de esta naturaleza no nos han producido más que algunos dolores de cabeza, pero son un síntoma de vitalidad en la red.[4]

A pesar del aumento de puertas para entrar en la red, hay que tener presente que aquella panda de hackers novatos no tenía más de 20 años, sin dinero ni experiencia en informática. Así que el mejor sitio para aprender y jugar gratuitamente con la red fue para muchos la universidad: pocos se licenciaron pues los aburrían las clases, no pasaron de los primeros cursos, pero estaban siempre como un clavo en el aula de ordenadores, aprendiendo por su cuenta. Víctor Huertas, responsable de seguridad informática de la Universitat Politècnica de Catalunya en 1996, dibujaba el perfil del hacker de aquella época: estudiante de informática o telecomunicaciones, entre 16 y 22 años, actuando en pequeños grupos de no más de cuatro miembros.[5]

Uno de estos chavales, de 19 años, explicaba a la prensa en 1997 las ventajas de la facultad: acceso a Internet y sistema operativo UNIX gratuitos y muchas horas para pasar ante el ordenador. La única pega era que, si te pillaban, te enfrentabas a la expulsión:

> -¿Qué es un hacker?
> -El que puede entrar en cualquier máquina.
> -¿Cuántas horas al día haces hacking?
> -De ocho de la mañana a ocho de la tarde, sin comer ni nada, a veces un bocata.
> -¿Y qué haces?
> -Buscar información para entrar en sistemas, contraseñas, programas...
> -¿Para hacer qué?
> -Para demostrar que el sistema educativo de la universidad no es bueno.
> -!!!
> -A mi no me gusta estudiar. Con el hacking, demuestras a la gente que puedes encontrar la información por ti mismo, que la puedes aplicar y que superas a los que han sacado muy buenas notas y están administrando un sistema.
> -¿Cuándo empezaste?
> -Cuando entré en la facultad de Informática de Barcelona, vi que sólo daban acceso total a Internet a los profesores y que los alumnos, como máximo, tenían correo electrónico. Tenías que buscarte la vida para conseguir un acceso de profesor.
> -¿Y después?
> -Empezamos a ampliar conocimientos: lo que hace un hombre, puede deshacerlo un hombre.
> -¿Empezamos?
> -Éramos dos, pero no trabajábamos juntos. Cada uno iba por su lado y poníamos cosas en común. También tenemos contactos con gente de Barcelona, Valencia y, pocos, de Madrid.
> -¿Y Estados Unidos?
> -No se puede hablar mucho porque los vigila la CIA. Nada más entrar en una máquina de allí, tienes a la CIA detrás.

-¿Alguna gesta heroica?
-He conseguido acceder a casi todas las universidades españolas, pero donde más me ha gustado estar ha sido el Centre de Supercomputació de Catalunya (CESCA).
-¿Por qué?
-Están muy orgullosos de ser invulnerables.
-¿Tienes ética?
-No tocar nada, no borrar nada... Y querría que toda la información fuese libre, sin ningún límite.**[6]**

1. HACKING/P/A/V/C:!Hispahack

!Hispahack, conocido también como **!H**, fue un grupo de hackers, la mayoría catalanes en sus inicios, activo entre 1993**[7]** y 2002. Son, sin lugar a dudas, los hackers más conocidos en España, debido al bombo y platillo mediático que acompañó la detención de algunos, en 1998. Cabe añadir que también fue uno de los grupos de más calidad del "underground" hispano.



!H nació en un canal de chat de Undernet que llevaba el nombre del grupo y que también frecuentaban miembros de Apòstols, La Vieja Guardia y otros aficionados al hacking, que a veces acababan siendo reclutados para el grupo, como le pasó a **Jfs**:

> Yo estuve desde 1995, me pescó SpeedFIRE tradeando shells en un canal de Undernet :-)**[8]**

Además de para charlar, el canal servía para intercambiar máquinas hackeadas, contraseñas y datos parecidos. Era un canal privado al que se entraba con contraseña. Uno de los miembros de !H, LeCréme, lo presentaba así a la prensa:

> Somos un grupo cerrado que incorpora gente esporádicamente, si tiene un cierto nivel y un interés por hacer cosas. Publicamos un "webzine", llamado "Mentas Inquietas", hacemos programas que ofrecemos al público, trabajamos en proyectos y intercambiamos conocimientos.**[9]**

Otros puntos más privados de reunión eran la BBS Twisted Reality, en Barcelona, y una lista de correo. La razón de la exclamación inicial en el nombre !Hispahack era salir los primeros en las listas de canales IRC de Undernet, como explicaba uno de sus miembros, de forma anónima, en un artículo publicado en el diario "El Mundo":

> ¿Por qué !Hispahack?, otra cosa sencilla, HISPA (Hispano) Hack (truco), en cuanto al símbolo de exclamación cerrada que le precede, la explicación es también muy sencilla: al ordenarse alfabéticamente la lista de canales que forman el IRC, la admiración hace que el canal !Hispahack salga el primero de la lista, ni más ni menos.**[10]**

1.1. Integrantes

!Hispahack tuvo muchos miembros, gente que entraba y salía y volvía. Fue

posiblemente el grupo más grande de la escena hacker española. Entre ellos **LeCrème** (LeC), **MindTwist**, **Zebal**, **BadreL**, **_J-R_**, **SpeedFIRE**, **Synflood**, **SEINA**, **Sage**, **vIERJa**, **Jamaro**, **Sylk**, **NandoL**, **EFE**, **Cure**, **y0man**, **Dorth**, **Slayer**, **Ludoz**, **Wait-Man**, **Sierra**, **Yandros**, **Stk**, **NetSavage**, **TaNiS**, **Flow**, **Renegade Master**, **Lethan**, **Jfs** (también llamado **Jafasa**), **Zhodiac**, **Drizzt**.

1.2. Mentes Inquietas

Como otros grupos, !H tenía su propio medio de comunicación pero, a diferencia del resto, que publicaban *ezines* (boletines electrónicos en formato texto que se descargaban de la web o se repartían en listas de correo), !H tenía una webzine (los artículos se publicaban en la web), llamada *Mentes Inquietas*.



Mentes Inquietas se puso en marcha en junio de 1997, a iniciativa de Lethan, y se alojó en el proveedor gratuito Angelfire. En la portada podía leerse el lema: *Lo único que nunca podrán quitarnos, son nuestras mentes. !H*. En su segunda época, se alojó en un servidor del Chaos Computer Club. De esta web se conserva copia en Internet Archive, a diferencia de la primera, que está totalmente desaparecida: Mentes Inquietas.

En la webzine publicaban miembros de !H y colaboradores de otros grupos o independientes. En su primera época (1997), firman artículos **sLMa** (Sociedad LiMitadisimA), LeCrème (LeC), Zebal, BadreL y **XXX**.

En la segunda época (1998-2001) escriben Flow, Renegade Master, Lethan, **GriYo**, Jfs, Zhodiac, Drizzt, **MiST**, **R.M.G.** y **Ansset**.

En *Mentes Inquietas* se publicaban programas y textos sobre clonaje de tarjetas, telefonía, fallos en Proveedores de Servicios de Internet, vulnerabilidades, exploits o colaboraciones con otros grupos, como The Hackers Choice.

De los programas creados y liberados gratuitamente por el grupo destacan *SmbScanner*, obra de Flow, que detectaba recursos compartidos e intentaba crackearlos; *Icmpush*[11], creado por Slayer, a partir del cual se desarrolló *Sing*, que hoy en día está en muchas distribuciones de GNU/Linux, o *HTTPush*, el primer

programa que permitía auditar aplicaciones web de forma interactiva y en cuya idea se basan la mayoría de proxies usados actualmente para este menester.

Entre los artículos de la primera época destaca un texto escrito por un anónimo, que más tarde se revelará como Carlos Sánchez Almeida, abogado especialista en delitos informáticos. Almeida firma un texto titulado Derechos del Detenido que en abril de 1998, cuando la Guardia Civil lleve a cabo una redada contra el grupo, le valdrá ser imputado -aunque rápidamente se retirarán los cargos.

El llamado *Caso !Hispahack* dio gran fama a este abogado, quien llevó la defensa de Jfs, el único integrante del grupo que tuvo que ir a juicio. Pero Jfs no fue el primer cliente "underground" de Almedia. Muy aficionado a los juegos, el abogado era asiduo a algunas BBS y conocía el mundillo, gozando de la confianza de la comunidad, que acudía a él cuando tenía problemas legales. Almeida había defendido ya a diversos phreakers, pero gracias al caso !Hispahack su fama saltó más allá del "underground" y en los años siguientes se le vio como abogado en los principales casos de hacking y P2P juzgados en el estado español.

1.3. Vocación internacional

Distingue a !Hispahack su vocación internacional. Sin ser un grupo admirado a nivel mundial, como lo fue 29A, destacaba su buena relación con otros grupos de hackers europeos, como The Hackers Choice o, especialmente, Chaos Computer Club.

hispahack.ccc.de

Gracias a esta buena relación, en enero de 1999 !Hispahack aparece en una selecta lista de grupos de hackers a nivel mundial: son los firmantes de la Declaración conjunta contra la ciberguerra. Los otros grupos son Cult of The Dead Cow, L0pht, Phrack, Chaos Computer Club, 2600 y los portugueses Toxyn y Pulhas.

En este manifiesto, el primero en la historia que publica una coalición internacional de grupos hacker, se condenan las declaraciones de otro grupo, Legion of the Underground (LoU)**[12]**, que había hecho una llamada a la ciberguerra contra los gobiernos de Irak y China. La coalición se oponía en el manifiesto a usar el hacking para realizar ataques contra países:

> Aunque estemos de acuerdo con LoU en que las atrocidades en China e Irak deben parar, no lo estamos con los métodos que quieren utilizar, que pueden ser muy contraproducentes. No se puede pedir legítimamente el libre acceso a la información de una nación, estropeando sus redes de datos. Si los hackers se ofrecen ellos mismos como armas, el hacking en general será visto como un acto de guerra.**[13]**

1.4. La segunda época

Hay un antes y un después del juicio del Caso !Hispahack, que marca muy claramente la vida del grupo. Desde las detenciones, en abril de 1998, hasta el juicio, en mayo de 1999, !Hispahack estuvo prácticamente parado. En el *Chaos Communication Congress* de 1998, el presidente del CCC, Wau Holland, pide la solidaridad de la comunidad internacional con !Hispahack, ante la criminalización de los hackers que está teniendo lugar en España**[14]**. Aparte de esto, no hay más alegrías para el grupo, que guarda silencio.

El 25 de julio de 1998, tres meses después de las detenciones, el servidor de la Guardia Civil está todo un fin de semana inaccesible. Algunos lo consideran la venganza de !Hispahack, pero representantes de la Benemérita niegan públicamente que haya habido un ataque. Diversos medios de comunicación reciben un mensaje, firmado por hacker@guardiacivil.org, quien reivindica el ataque a los servidores principal y de correo del cuerpo.

En diciembre de 1998, la web de la Guardia Civil es redirigida a una página con información para homosexuales, después que un atacante ha cambiado los servidores de nombres del dominio guardiacivil.org por ns1.gay.com y ns2.gay.com**[15]**. Cara al público, la Guardia Civil se lo toma a broma.**[16]**

No será hasta después del juicio que se vean movimientos constructivos en !H. Abren una nueva web, alojada en el servidor del CCC y publican en su webzine la existencia de una vulnerabilidad en el servidor web de la Guardia Civil.**[17]**



En noviembre de 1999, aproximadamente medio año después del juicio que lo absolverá, Jfs se da el gusto de volver a ser noticia, pero por algo positivo: gana un difícil concurso de hacking de la revista *PCWeek***[18] [19]** y publica un artículo explicando cómo lo hizo: "A practical vulnerabilty analysis (the PCWeek crack)"

1.5. Jugando a la guerra

En 1999, algunos miembros del grupo aparecen en un reportaje del programa de Televisión Española "Documentos TV": *Internet, Zona Peligrosa***[20]**. Es el primero en televisión que retrata con fidelidad a la escena hacker y ha sido grabado, en parte, durante la primera edición de la NoConName. Allí, la empresa *Com & Media* (actualmente S21sec), patrocinadora de la *con*, ofrece trabajo a algunos asistentes, entre ellos Zhodiac, recién llegado a !H.

En los siguientes meses y años *Com & Media* fichará a otros miembros del grupo, que al entrar en el mundo profesional se quedarán con poco tiempo para dedicar al hacking, además que sus contratos les obligarán a no hacer públicas sus investigaciones. Esto es la muerte para cualquier grupo de hacking, también para !Hispahack.

El capitán de esta última época es Lethan, que intentará en vano mantener vivo al grupo, convirtiéndolo en asociación, idea que no cuajará. Mientras, !H aumentará su agresividad, siendo conocido más por sus enfrentamientos que por sus logros: se encona la lucha con su eterno rival, SET, y hay diversos enfrentamientos contra la asociación Infohackers **[21]**, incluso se crea un frente común de grupos que firman un manifiesto**[22] [23]** desautorizando a esta asociación: Kernel PaniK, !Hispahack, PhonePhreakPhun, 7a69 ezine, CPNE, Akelarre, Undersec, TDD y t0s.

A partir de mayo de 2001 no aparecen nuevos artículos en *Mentes inquietas*. Más adelante sólo hay noticias de problemas entre algunos miembros del grupo. El 16 de enero de 2004 aparece en algunos blogs la noticia de que Hispahack se ha disuelto y hay una nota en la web del grupo:

> Lamentablemente no hemos podido plataformar este proyecto adecuadamente, faltan apoyos y una persona sola no puede tirar del carro, más cuando sus responsabilidades profesionales le roban todo el tiempo.
>
> Ahora lucharemos desde otra trinchera, personalmente seguiré en una organización sólida como el Chaos Computer Club, y en activo como profesional dedicado a la seguridad.
>
> Es triste, pero lamentablemente en España la sociedad demanda hackers de circo y es algo difícil de cambiar.
>
> Saludos,
> Albert**[24]**

TaNiS, un histórico de la comunidad hacker, forjado en La Vieja Guardia, acompañó a Lethan en este final:

> Junto a Lethan, fui el último en dejar !H, alrededor de 2004-2005. A Lethan le tiraba más el Chaos Computer Club y ya no había nadie que quisiera mantener viva la llama, por malos rollos, etc.**[25]**

En fecha indeterminada, Zhodiac volvió a subir a Internet la vieja web de !Hispahack.

2. H/PHREAKING/A/V/C: CPNE

CPNE eran las siglas de la Compañía Phreaker Nacional de España, también llamada Compañía de Phreakers Nacional de España y Compañía de Phreaking Nacional de España. La CPNE no era un grupo sino una web, creada a principios de 1997, que funcionaba como directorio de información sobre phreaking.



Logotipo de CPNE

Su creador fue el polifacético **WaReZZMaN**, autor también de la web Iberhack, nacida en 1996 y una de las primeras que ofrecía enlaces sobre hacking en castellano**[26]**. Junto a Warezzman estaba **Dark Raver**. Ambos fundaron también la revista Saqueadores Edición Técnica (SET)**[27]** y la primera convención anual de la escena hacker española, Undercon.

Eran de Murcia o alrededores y su influencia en el hacking hispano es innegable. Ellos e !Hispahack eran los grupos *élite* y sus fundadores mantenían relaciones cordiales. Fue más adelante, con la llegada de nuevos integrantes a ambos colectivos, que lo que hasta entonces podía ser una natural y sana competencia entre grupos se fue convirtiendo en rivalidad, hasta escenas vergonzantes cómo el deface de la web de SET, que se contará más adelante.

Pero igual como la vida es una rueda que vuelve al punto de inicio, cuando moría la escena hacker de los 90 nació un nuevo grupo, The Old School (t0s), que duró de 2002 a 2004 y en el que se refugiaron, sin peleas, viejos miembros del *clan murciano* y de *los catalanes*: **Dark Raver** (de CPNE y SET), **Jfs** y **SagE** (de !Hispahack), **Fuego Fatuo** (La Katedral y CPNE), y **IaM**.

Volviendo a los murcianos, junto a Warezzman y Dark Raver hubo siempre colaboradores de peso, que iban cambiando de *nick* pero no necesariamente de cara. En la aventura de la CPNE estaban **FastData** y **PaTiLLas[28]**. Más adelante se les unió Fuego Fatuo, procedente de La Katedral, el grupo-cantera de CPNE.

El nombre, así como el logo de la CPNE, era un remedo de su principal víctima: la

Compañía Telefónica Nacional de España, que ostentaba el monopolio de la telefonía en España. La principal misión de la CPNE era el phreaking o hacking de las líneas telefónicas.

> La CPNE es una iniciativa de warezzman (...) ante las carencias en el mundillo del phreaking en España.
>
> Estas carencias suelen ser:
> - La falta de información valida en España (muchas boxes pero para USA)
> - La falta de información actual sobre Telefónica
> - La dificultad de encontrar la poca información de calidad que hay
> - La falta de organización entre los pocos phreakers en España
>
> La CPNE pretende ser una especie de base de datos sobre el sistema telefónico español y las experiencias de los phreakers españoles.**[29]**

La web de CPNE nació en Geocities tuvo diversos espejos en sitios gratuitos, uno de ellos en Isla Tortuga: cpne.islatortuga.com, abierto en mayo de 1997 y actualizado por última vez en febrero de 1998.

2.1. Contexto

El phreaking había nacido en los años 50 en Estados Unidos y las primeras blue boxes o cajas azules (dispositivos para llamar sin pagar) se construyeron en los 70.**[30]**

> La caja azul o la caja negra, que usando la señalización de control de la red de telefonía permiten hacer llamadas gratis, añadir crédito a una cabina pública sin introducir dinero, hacer que suene el teléfono aunque no haya ninguna llamada, falsificar la identidad de una llamada, etc... Aparte de esto, se atacaron los sistemas de prepago, la seguridad física de las cabinas públicas, modems conectados a la red telefónica, etc, etc...**[31]**

En España el phreaking llegó más tarde, a finales de los 80, con el auge de las BBS. Las razones son dos: por una parte, la información para aprender a realizar esta actividad se replicaba a través de las BBS. Por otra parte, acceder a ellas significaba tener que usar el teléfono de forma intensiva, más teniendo en cuenta la lenta velocidad de los módems. Los hackers adolescentes no podían pagar las elevadas facturas que generaban sus llamadas, así que llamar gratis era vital para ellos.

Una de las actividades más importantes de los primeros grupos españoles conocidos, Glaucoma y Apòstols, fue el phreaking. EnderWiggins, miembro de Apòstols, había escrito el primer manual en castellano, el Manual del Novicio al hack/phreack, donde se daban detalles sobre cómo construir cajas azules y negras que funcionasen en el sistema telefónico español, diferente al norteamericano, lo que provocó que se crease una “box” a medida: la “Mahou Box”, una caja negra que permitía llamar sin pagar en España.

> La Mahou box es una caja diseñada en espain y para usarse aqui. (...) Lo que hace esta caja es anular esa se¤al de 12kh que activa los contadores de pasos ya sabes(Eh! Antonio, dale al chisme que voy a llamar a casa pa’ decir que voy a llegar tarde,ah y ponme otra cañaa).Asi cuando el aparatejo no haya saltado porque no le ha llegado ningua se¤al, no te cobraran

nada.[32]

A partir de 1995, con la llegada de los primeros proveedores de Internet que multiplicó el número de usuarios de Internet y cuando aún no existía la tarifa plana telefónica, la necesidad de usar el teléfono sin pagar se hizo extensiva a una parte más amplia de la población. Entonces nace el *movimiento phreak*, la época dorada del phreak español, cuando se ampliará de forma importante la investigación en el sistema telefónico español, incluidas las cabinas públicas, con el objetivo prioritario de llamar gratis y anónimamente.

En este contexto nacen diversos grupos dedicados a la investigación, junto a páginas web que replican la información descubierta. La web de la CPNE es la primera dedicada íntegramente a ofrecer documentación propia -y también ajena-sobre phreaking. En cuanto a los grupos de phreakers, destacan La Katedral, Net Phreak Team (en realidad un proyecto personal, del madrileño OverDrive), The Den of the Demons, Esphreak y Akelarre.

> Cada uno de estos grupos tendió a especializarse en un campo especifico, NPT ofrecía importante información sobre los primeros fallos de las operadoras de GSM, mientras que la CPNE se definían en su propio web como "apasionados del sistema telefónico, investigadores de las telecomunicaciones, que tienen por hobby conocer el funcionamiento de las redes de telefonía" en sus páginas se podían encontrar múltiples información técnicas de los sistemas de Telefónica, algunos de los cuales podían ser empleados para acceder a sistemas internos o evitar la tarificación de las llamadas. Los TDD, también apodados los "McGyvers del Phreak". Fueron los que descubrieron cómo llamar gratis desde las cabinas telefónicas usando como única herramienta la chapa de una lata de refrescos.[33]

A partir del año 2000 el phreaking español bajó de intensidad, debido a la llegada de tarifas planas para acceder a Internet, la bajada del precio de las llamadas interprovinciales e internacionales, el fin del monopolio de Telefónica y la mayor persecución policial de las prácticas de phreaking. En los años 90, diversas personas habían sido detenidas por llamar sin pagar, siendo la práctica más popular usar la línea de pruebas que Telefónica tiene en todos los edificios. Como no estaba aún tipificado este delito, se les acusaba de *fraude de fluido eléctrico* que solía condenarse con multa, sin penas de prisión. La Operación Millenium puede considerarse el último gran acto público del phreaking español, una macro redada que acabó con la detención de 55 personas, por uso fraudulento de números gratuitos 900.

2.2. El phreaking según CPNE

La mayoría de usuarios del phreaking, los que leían las webs y ponían en práctica las informaciones allí contenidas, lo hacían para llamar gratis, sin plantearse nada más allá. Pero quienes investigaban las redes telefónicas -los auténticos phreakers-sí tenían algún tipo de posicionamiento moral o filosófico. En la web de CPNE había una definición de phreaker, posiblemente escrita por Warezzman, que es también una declaración de principios:

> Un phreaker es un apasionado del sistema telefonico, un investigador de las

telecomunicaciones, su hobby es conocer el funcionamiento de de las redes de telefonia. Aveces emplea este conocimiento jugar con el sistema y hacer cosas como desviar llamadas, pero ese no es su fin principal. Otras veces usa la informacion para llamar gratis pero lo hace por que piensa que las telecomunicaciones son un servicio basico como la sanidad o la educacion y deberian ser algo gratutito y no un chollo para unos pocos. Las comunicaciones si son un bien de interes general y no el Futbol.[34]

2.3. Investigación propia

El sitio web de la CPNE era un repositorio de dos tipos de información: la generada por su equipo de I+D y la recopilada de otras fuentes. En un principio, sólo se publicaba información no propia, dado que el objetivo prioritario era aportar datos a la comunidad sobre el sistema telefónico español. Pero pronto se vio necesario ampliar esta documentación con investigación propia.

> Gran parte de los objetivos que nos planteamos al comenzar esta andadura se han cumplido y estamos orgullosos de haber colaborado en gran medida en la expasion y crecimiento del phreak latino. Actualmente CPNE tiene una doble vertiente: El grupo CPNE que se dedica a la I+D y a la produccion propia de documentacion, software y elementos hardware.[35]

Warezzman era el encargado de investigación y desarrollo, mientras que Fastdata y Patillas funcionaban como "comando de asalto" cuya función era obtener información mediante ingeniería social, trashing y otros[36]. Warezzman explicaba a un periodista de la revista "iWorld" cómo realizaban sus investigaciones:

> "La ingeniería social es bastante práctica con los técnicos, tanto físicamente como por teléfono, pero totalmente inútil con comerciales y operadoras, pues no suelen tener ni idea de telefonía, comunicaciones o el sistema que usa su propia compañía (...), a veces he acabado yo explicándoles a ellos las cosas", aunque matiza que "por teléfono se obtienen pocos datos, es mejor en persona, a través de conocidos que trabajen en Telefónica, el técnico que viene a casa, esas cosas. Mostrando un poco de interés por su trabajo (...) se pueden extraer cosas jugosas". Otra forma de hacerse con información es el "basureo": estar al acecho de lo que ciertas empresas tiran a la basura. (...) Es el método mediante el que warezzman consiguió hacerse con piezas de una centralita Pentaconta-32 de Telefónica.[37]

A estas tareas de investigación se añadía la figura del colaborador, que sin formar parte del grupo podía aportar textos. A cambio, recibía acceso a información privilegiada y tenía entrada a los canales de chat y listas de correo del grupo. **Mad Hacker**, **Merlin** y **mwarez** colaboraron con diversos tutoriales y artículos en la web de CPNE.[38]

CPNE contó también con la ayuda puntual de otros hackers, como **LeCreme** (Hispahack) o **Wendigo**, del Sindicato de Hackers Españoles, a quienes se agradece su colaboración para crear las Páginas Grises '97. Así, CPNE acabó siendo un compendio exhaustivo e imprescindible para la comunidad:

> Desde como funcionan las tarjetas de prepago, los fallos de las cabinas para llamar gratis, como hacer llamadas gratis con Movistar a través del programa Vomistar (esto es nuevo),cambiar las propiedades de los móviles, etc... y para eso los modelos OKI900 o Motorola executive, son los más utilizados para ello, ya que según tengo entendido solo se ha de hacer un puente en algun contacto para escuchar conversaciones con, desde y hacia MoviLine, o como a través de tarjetas telefónicas, hacer llamadas a costa de otros, o incluso realizar el

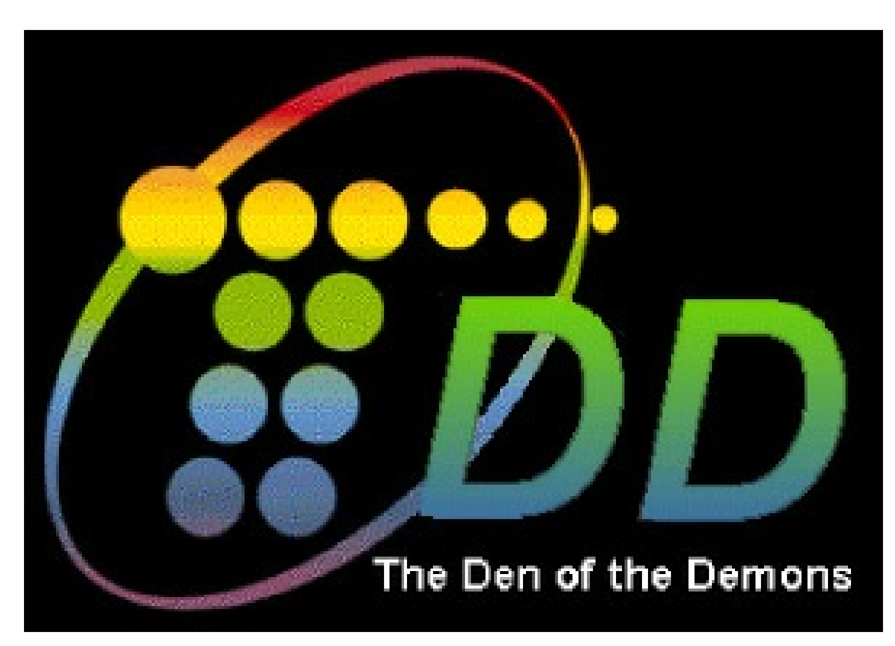
beife boxing, osea pinchar un telefono, osea con eso cuidadin que puedes ir al trulling!!![39]

2.4. La escena phreak: The Den of the Demons

Queda muy poca información sobre los grupos que aportaban información a CPNE y que formaban la escena del phreak. Es sabido que había fuertes vínculos entre La Katedral y CPNE, pues algunos de los miembros del grupo estaban también en CPNE, hasta que La Katedral murió.

> KTD se dejaron de hacer cosas porque éramos una mezcla de gente que controlaba más y gente que sólo estaba para pillar los 900s.[40]

Los números 900 eran teléfonos de empresas, muy buscados porque permitían entrar a Internet sin pagar. En cuanto al resto de grupos, **The Den of the Demons** es el único del que se conserva información pública, y no mucha, en Internet. Fue muy activo en el área de las cabinas telefónicas.



El grupo nació en verano de 1997, según contaba uno de sus miembros, **Armand VanHell**, en una entrevista en la revista SET:

> Al principio empezamos **Hark** y yo con ciertas experiencias que desembocaron en querer saber mas sobre esos “cacharros” que estan en las calles llamados normalmente cabinas y mas en concreto los TM (Telefonos Modulares). Luego al poco se unio **Ripper** para apoyarnos en ciertas cuestiones. (...) Y asi los 3 mosqueteros llevamos unos a~os danzando por ahi como los monos en el arbol del phreak.[41]

Se les apodaba “los McGyvers del Phreak”[42]. El acrónimo de su nombre, TDD, es también un acrónimo usado en telecomunicaciones que significa *Time-Division Duplexing*.[43]

2.4.1. Chaping



Cabina de la época

Queda poca información en Internet de las investigaciones del grupo, al haber desaparecido su sitio web. Uno de sus textos más conocidos que aún se conserva explica cómo hacer llamadas con cargo a la compañía Telefónica, usando para ello su especialidad: una cabina, e ingeniería social.**[44]**

Entre los hacks más famosos de TDD destaca el *chaping*, que permitía llamar gratis desde una cabina usando la chapa de una lata de refrescos. Consistía en llamar a un número gratuito y, cuando se establecía la conexión, se cortaba con una chapa. El grupo lo presentó oficialmente en la segunda edición de la Undercon, en 1998**[45]**. Posteriormente, la revista Raregazz publicó una revisión del texto, firmada por Armand VanHell**[46]**. Más adelante TDD automatizó este truco con la llamada *chaping card*.

Otro descubrimiento del grupo fue cómo reiniciar las cabinas telefónicas**[47]**, que de hecho era necesario para la práctica del chaping.



Fuera de Servicio

> Otra anécdota publicada por primera vez por TDD, que a día de hoy aun funciona al menos en cabinas de la (T) e incluso otros operadores, como ONO, es dejarlas fuera de servicio sin fuerza. Descolgar el telefonillo - Pulsar [R] y si no tuviera [R] el asterisco tambien vale - colgar con la mano - Volver a descolgar. Aparecerá un mensaje de Fuera de servicio. A los 2-3 minutos la cabina se resetea sola**[48]**

TDD también creó una tarjeta de teléfonos recargable que sería muy popular, el

Emulador de Tarjetas de Telefónica, con un microcontrolador PIC16F84A[49] y una resistencia. El emulador generaba el código de serie de las teletarjetas de Cabitel y hacía creer a la cabina que estaba ante una tarjeta auténtica.

> Incluso el botón de cambio de tarjeta funcionaba, se sacaba y se volvía a introducir. Algunas cabinas perdían voltaje, se reseteaban, pero fueron problemas menores.[50]

2.4.2. Divulgación en la UnderCon

Buena parte de la investigación llevada a cabo por TDD se ha conservado gracias a que la divulgaron en la UnderCon, que las publicó en su web. En la UnderCon de 1998, además de hablar sobre el *chaping*, ofrecieron una *"Descripción del recorrido que lleva a cabo la línea del teléfono"*[51], texto que recopiló también el sitio documental Prehackers y ha conservado Internet Archive[52]. En aquella edición de la Undercon, Ripper firma una crónica, como miembro de TDD.[53]

```
                  TDD
                 ^^^^^
         The Den of the Demons
Phreak Rulez!   Group of Phreakers   Phreak Rulez!

          http://www.webcrunchers.com/tdd
          http://www.thepentagon.com/tdd
          http://pagina.de/tddz

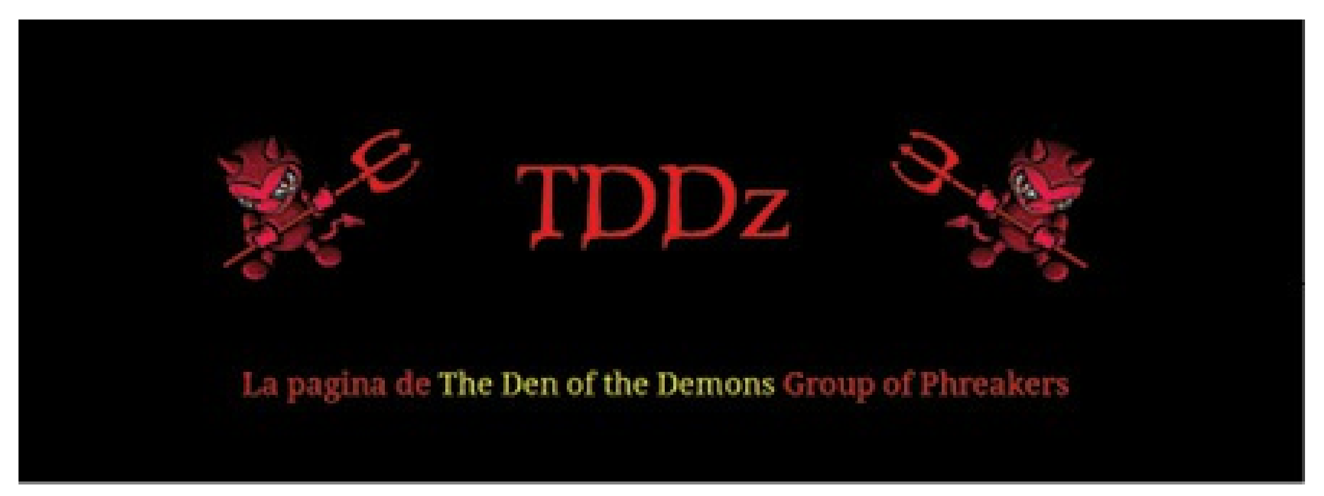
  NOMBRE DEL FICHERO: Que te puedes encontrar en un 900? (under00.txt)
  AUTOR: Hark
  ULTIMA REVISION: 12/10/2000 v1.0

Texto recomendado para EDIT de MS-DOS. Documento obtenido del grupo TDD.
  NO DISTRIBUIR -+- NO DISTRIBUIR -+- NO DISTRIBUIR -+-  NO DISTRIBUIR
```

El grupo dio charlas también en la Undercon 2000: *"Que te puedes encontrar en un 900?"*, firmado por Hark[54], y en la Undercon 2004: *"Seguridad Fisica en un TM"*, firmado por TDDz y ^Oscuritoz.[55]

Como expertos que eran en phreaking, TDD se metieron también en el mundo de las "boxes" o aparatos que ayudan a realizar llamadas gratuitas. Concretamente, se conserva un texto de TDD sobre las "beige boxes", para llamar gratis conectándose a los postes telefónicos y al par piloto:

> Ya esta! con el PLAN Beige & Family de TDD podras llamar a tropecientos numeros con un 100% de descuento XD.[56]



La web oficial de TDD se alojaba en Isla Tortuga, en la dirección tdd.islatortuga.com, pero no queda ningún vestigio de la misma. También estuvo en www.webcrunchers.com/tdd, igualmente desaparecida aunque conservada en parte gracias a Internet Archive.[57]

No se conoce la fecha de desaparición del grupo. Posiblemente coincida con el último vestigio de la web de Webcrunchers, en 2004.

3. H/P/A/VIRII/C: 29A

29A fue un grupo de hackers especialistas en escribir virus por amor al arte. Nació a finales de 1995 y murió en febrero de 2008. Aunque surgió en España y siempre tuvo miembros españoles, contó entre sus filas con destacados expertos de otros países. Es considerado uno de los mejores grupos de programadores de virus del mundo debido a sus originales investigaciones y alta calidad técnica, que les llevaron a escribir algunos de los virus más innovadores de la historia. Entre otros, destacan el primero para Windows de 32 bits, el primero multiplataforma, el primero que funcionaba en Linux y Windows y el primero para teléfonos móviles. Los daban a conocer a través de la revista del mismo nombre.



El nombre del grupo y la ezine, *29A*, es la representación hexadecimal del número "666" en el sistema decimal. A pesar de esta referencia satánica, 29A destacó por su ética en la creación de virus, a los que consideraba vida artificial fascinante por sí misma y no por los ordenadores que pudiese infectar, como resumía en una frase uno de sus miembros, Mental Driller: *"Prohibido el código destructivo y se programa por afición y placer, no por fastidiar a la gente"*.**[58]**

Además de la BBS Dark Node, donde nacieron, el grupo se comunicaba en una lista de correo interna y un canal de IRC. Algunos de sus miembros se movían también por los canales #hack, #viruslatin y #virus de EFNet, #virus y #hack de IRC-Hispano, #vir, #virus, #vxers y #asm de Undernet, alt.comp.virus y otros foros habituales de los amantes de los virus.

En sus inicios, el grupo se citaba también físicamente: tres veces al año en Santiago de Compostela o Madrid, según cuenta su primer líder **MrSandman**, en una entrevista de presentación de 29A**[59]**. A uno de estos encuentros, la primera quedada en Madrid, asistió el experto en virus Bernardo Quintero, en verano de 1997:

> En la quedada física que hicieron en Madrid estuvimos en varios sitios (almorzando, por la noche de botellón, etc), pero una tarde se pasó en el parque de atracciones de Madrid. Mientras esperábamos cola en una atracción, uno de ellos llevaba impreso en la espalda un

volcado hexadecimal de un virus (sólo valores hexadecimales), y dos de ellos que iban tras él, aburridos, se pusieron directamente a hacer la traducción a ensamblador sobre la marcha a viva voz y a interpretar directamente lo que hacía el bicho como quién lee un libro.... yo flipaba (cualquier humano, incluido yo que me movía en ese mundillo, necesitaba un ordenador, un desensamblador, y echar un buen rato para hacer algo parecido).**[60] [61]**

Sus miembros, muchos de ellos programadores de virus reconocidos mundialmente, fueron: **Mister Sandman**, **Anibal Lecter**, **AVV**, **Blade Runner**, **Gordon Shumway**, **Griyo**, **Leugim San**, **Mr. White**, **Tcp**, **The Slug**, **VirusBuster**, **Wintermute**, **Darkman**, **Jacky Qwerty**, **Rajaat**, **Reptile**, **Super**, **Vecna**, **Mental Driller**, **SoPinky**, **Z0mbie**, **Benny**, **Bumblebee**, **LethalMind**, **Lord Julus**, **Prizzy**, **Mandragore**, **Ratter**, **roy g biv**, **Vallez**.

3.1. Dark Node



Ordenador donde residía la BBS Dark Node

29A nació en la BBS Dark Node, dedicada a la investigación vírica y donde había foros de debate sobre este tema. Propiedad de VirusBuster, Dark Node estaba físicamente en Villagarcía de Arosa (más tarde se trasladó a Santiago de Compostela). Era punto de reunión habitual de los principales expertos españoles en virología informática.

Formaba una red tipo Fido en la que el nodo principal, Dark Node, tenía como dirección 66:666/1, así que por ahí vienen los tiros en cuanto al origen del nombre del grupo.**[62]**

Mister Sandman, quien lideró el grupo en sus inicios, conoció a VirusBuster y Gordon Shumway en el área sobre virus de FidoNet. Pero, debido al mal ambiente que había allí, según cuenta Sandman, VirusBuster y Shumway crearon la BBS Dark Node en abril de 1995 e invitaron a algunos especialistas en virus a visitarla. Así fue como los primeros miembros de 29A entraron en contacto y empezaron a intercambiar información, analizar virus y buscar fallos en antivirus.

Como otras BBS, Dark Node tenía diferentes niveles de acceso: desde sólo poder escribir un mensaje en los foros público hasta acceder a zonas especiales, privilegio de unos pocos que eran llamados élite. A finales de noviembre de 1995, Mister Sandman propuso a algunos componentes de esta élite crear un grupo organizado

de escritores de virus y, dado que habían generado suficiente información en los últimos meses, recopilarla en forma de artículos y hacerla pública a través de una revista.

> De esta forma, sacarían partido al trabajo que llevaban desarrollando durante meses (artículos, virus, desensamblados..), recopilarlo en una e-zine y así poder rivalizar con los dos grupos de escritores de virus más importantes en aquel momento: VLAD e Inmortal Riot.**[63]**

La idea cuajó y el 13 de diciembre de 1996 (viernes 13), salía el primer ejemplar de la revista 29A.**[64]**

3.2. Contexto

29A fue el único grupo español, estable y conocido públicamente, que se dedicó a la creación de virus, lo que llevó a Mister Sandman a decir: *"La escena en España es 29A"***[65]**. A nivel internacional, 29A había nacido como un grupo normalito, uno más. Pero pronto destacó hasta ser considerado uno de los mejores, si no el mejor.

La primera ezine sobre virus en el mundo había nacido en 1991, de la mano de Hellraiser y Bionic Slasher. Se llamó "40Hex"**[66]** y su contenido eran artículos donde se enseñaban códigos fuente de virus interesantes, técnicas para que un virus esquive a los antivirus, etc.

> 40Hex alcanzó inesperadas cotas de popularidad, tanto que un mes después, con la llegada de cuatro escritores más, se creó Phalcon/Skism, considerado hoy día como el primer grupo de escritores de virus organizados. La e-zine 40Hex siguió revolucionando la "virus scene", hasta agosto de 1995, cuando lanzaron su 14 edición y dejaron de dedicarse al mundo de los virus.
>
> A partir de entonces, tuvo lugar una auténtica vorágine de apariciones y desapariciones de grupos de creadores víricos, como NuKE, Immortal Riot, YAM, los argentinos DAN o los australianos VLAD. Estos últimos han sido los más importantes, ya que fueron los que inventaron la infección de ficheros NewEXE y PE (formatos de ejecutables nativos de Windows 3.1 y Windows 95, respectivamente) y otras plataformas, como Linux, y gran cantidad de técnicas totalmente desconocidas y novedosas (el virus Bizatch o Boza, el primero específico para Win95).**[67]**

Cuando nació 29A, en 1995, acababa de aparecer otro grupo, IR/G, fruto de la fusión y decadencia de Immortal Riot y Genesis. También VLAD iniciaba su declive, debido a la retirada de sus hombres fuertes Qark y Quantum. IR/G no aguantó mucho. Esto, explica Javier Guerrero en PCManía, *"deja a los españoles prácticamente al frente de la "scene"*.**[68]**

En el primer número de la ezine de 29A, Mister Sandman se refiere a este contexto en el que nace el grupo:

> Somos parte de la escena virica que se está regenerando continuamente. En los últimos tiempos hemos podido ver cuántos grupos han aparecido, se han fusionado o muerto. Thus, Qark y quantum se han retirado y disfrutan la vida, SVL se disolvió debido a problemas legales en Eslovaquia, Immortal Riot y Genesis se fusionaron y están a punto de sacar su primer número en las próximas dos semanas, Dark Conspiracy desapareció pero muchos de sus miembros fundaron un nuevo grupo, LT, que se fusionó con RSA, iKs ha sacado su

> primera ezine... como puedes ver, esto no para de moverse.
>
> Incluso hay un nuevo grupo, Computa Gangsta, que han sacado recientemente el primer número de su ezine, DHC, y parecen querer seguir los pasos de YAM... ¡o peor! **[69]**

3.3. Vida pública/Ezine

3.3.1. Issue # 1/Viernes 13, 666, los 12 magníficos

La primera ezine de 29A aparece el viernes 13 de diciembre de 1996, a las 6:66 am (7:06). Se llegarán a distribuir 10.000 ejemplares por todo el mundo.

> Incluimos algunos tutoriales (polimorfismo, virus de macro...), técnicas virales (cómo deshabilitar algunos AVs, chequeos de instalación nueva...), desensamblajes de algunos virus (Zhengxi, V.6000...) y virus escritos por nosotros, por supuesto :) Echad un vistazo al índice de virus, porque algunos son realmente interesantes y/o innovan con nuevas técnicas nunca usadas hasta ahora.**[70]**

El staff de 29A en este primer número lo forman: Mister Sandman, Anibal Lecter, AVV, Blade Runner, Gordon Shumway, Griyo, Leugim San, Mr. White, Tcp, The Slug, VirusBuster y Wintermute. Son todos españoles, algo que no volverá a repetirse. Los virus propios que presentan son: **Torero** (MrSandman), **Internal Overlay** (Tcp), **Cricri** (GriYo), **TheBugger** (The Slug), **Apocalyptic** (Wintermute), **AVP-Aids** (Tcp), **AntiCARO** (MrSandman) y **Galicia Kalidade** (Mad Mother Team).

3.3.2. Issue # 2/La nueva escuela Win32

El segundo número aparece un año después, el viernes 13 de febrero de 1998, a las 6:66 pm. En la presentación, Mister Sandman achaca la espera de un año a reestructuraciones internas, algunos miembros haciendo el servicio militar y, lo más importante, asegura: *"La necesidad de gastar mucho tiempo en trabajo de I+D para empezar el camino en la llamada "nueva escuela" (Win32)"*.**[71]**

La ezine está repleta de alta calidad y buenos virus de creación propia: infectores para Win32, el primero multiplataforma (Esperanto, escrito por MrSandman), el primero que se ejecuta al revés, el primer infector de arranque que usa características PMODE, el más extendido en el mundo en aquel momento (CAP, de Jack Qwerty) y otros.

El grupo tiene una web oficial en Isla Tortuga, *29A Labs*: 29A.islatortuga.com y ha abierto un canal de chat, #virus, en la red española IRC Hispano. Mucha gente se acerca al grupo, españoles y extranjeros, algunos con intención de unirse a él. Así que deciden crear una nueva figura: el colaborador, que no es miembro oficial, pero puede escribir artículos y virus para colaborar con la ezine y el grupo.

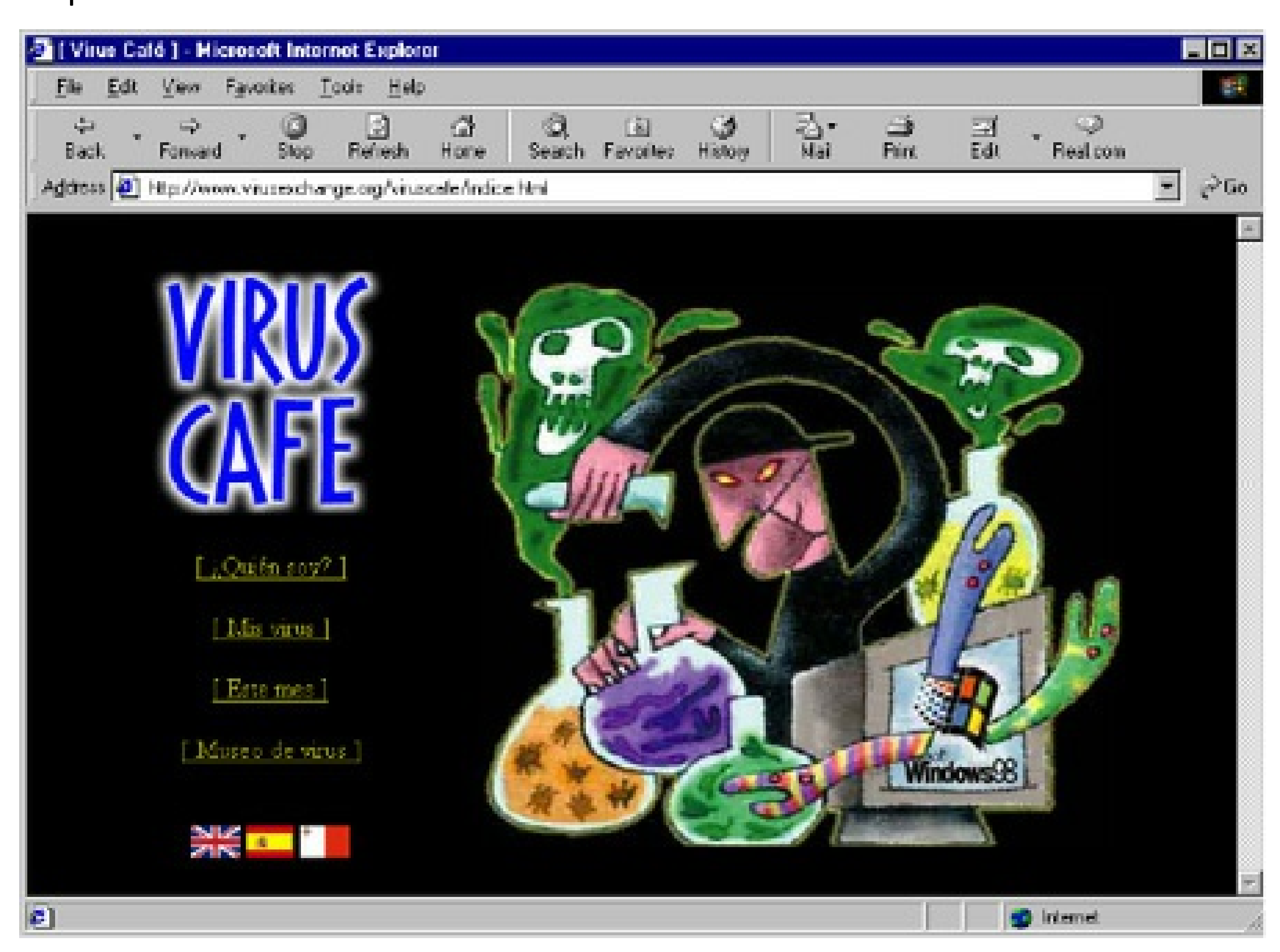
El staff de 29A en 1998, al que Sandman llama el "VX dream-team", cuenta con nuevas incorporaciones, algunas de fuera de España: Mister Sandman, Darkman (nueva incorporación, de Holanda), GriYo, Jack Qwerty (nueva incorporación, de Perú), Rajaat (nueva incorporación, de Gran Bretaña, ex-IR/G)**[72]**, Reptile (nueva incorporación, de Canadá), Super (nueva incorporación, de España), Tcp, Vecna

(nueva incorporación, de Brasil) y Wintermute.

3.3.3. Issue # 3/MrSandman se va en pleno apogeo

La tercera edición de la ezine aparece a finales de 1998. La noticia más importante es que Mister Sandman deja 29A, por cuestiones personales[73] aunque se rumorea que hay problemas internos con otro miembro del grupo. También lo dejan Wintermute y Rajaat[74]. La despedida de Wintermute puede leerse dentro del código del virus Ithaqua.[75]

Por otra parte, entra gente nueva en el staff: Mental Driller (España), SoPinky (Argentina), VirusBuster (España) y Z0mbie (Rusia). Se anuncia un nuevo canal de chat para estar en contacto: #vir en Undernet.



Después de dejar 29A, Mister Sandman creó su propia web: VirusCafé



Virus creados por Mister Sandman

En julio de 1998, 29A ha sido anfitrión en Madrid de una reunión del foro Virus Exchange y se publica la crónica en esta ezine:

> Nombro a los asistentes y espero no olvidar a nadie: fuimos Spanska, Darkman/29A, Tcp/29A, Reptile/29A, Super/29A, B0z0/IkX, StarZero/IkX, GriYo/29A, Wintermute/29A, MrSandman/29A, VirusBuster/29A, Mental Driller/29A, Binaria&DarkNail (dos hackers españoles), Ic¡ar (hi!), tres periodists de una importante revista española y las novias de GriYo, Sandman, Virusbust y Darkman.[76]

También en este número se anuncia la creación, a mediados de 1997, de un nuevo grupo de escritores de virus españoles: DDT, formado por zAxOn, dustfaery, Frontis, The Wizard, mandragore y Billy Belcebu[77]. El cofundador de 29A, VirusBuster, será miembro de DDT durante unos días, para volver después a 29A. El grupo no durará mucho tiempo: en marzo del 2000 se anuncia su muerte.[78]

3.3.4. Issue # 4/Días de vino y rosas

En febrero/marzo del año 2000 aparece la cuarta edición de 29A, repleta de artículos y especímenes, con nuevas incorporaciones[79] y gente que se va. Llegan Benny (República Checa)[80], Bumblebee (España)[81], LethalMind (Francia), Lord Julus (Rumanía)[82] y Prizzy (República Checa)[83]. Se van Jacky Qwerty, Vecna y Z0mbie.

La web del grupo ha cambiado por enésima vez de sitio y está ahora en: coderz.net/29A

Llama la atención la gran cantidad de trabajo que trae este número: 32 artículos, 6 herramientas, 9 gusanos, 28 virus para Win32, 18 para Win9x, 12 para DOS y 6 para RISC OS y UNIX: en total, 73 piezas. Benny y Darkman presentan el **Win2000.Installer**, el primer virus para el sistema operativo Windows 2000, cuando aún no se ha presentado oficialmente este sistema operativo.[84]

3.3.5. Issue # 5/¿Mucho ruido y pocas nueces?

En diciembre del 2000 sale el quinto número[85] de la ezine. Edita VirusBuster. Abandonan el barco Darkman, Lethal Mind, Reptile, Sopinky, Bumblebee y Prizzy, dejando el staff con menos miembros de la historia de 29A: Benny, GriYo, Lord Julus, Super, Tcp, The Mental Driller y VirusBuster. Se une a ellos el francés Mandragore.

Es un número cargado de artículos y piezas de código vírico, mayoritariamente para el sistema operativo Windows. Un colaborador, MaskBits, publica el código del primer troyano para PHP, **Pirus.**[86]

Se informa sobre un encuentro local de la escena vírica en octubre, en Valencia, al que asisten Billy Belcebu, The Mental Driller, Tcp, Super y Bumblebee, entre otros. En verano se ha celebrado el encuentro internacional en la ciudad de Benny, Brno, en la República Checa, de la que también se informa en la ezine y que ha sido menos concurrida que la cita valenciana.

3.3.6. Issue # 6/La decadencia de la escena vírica

Marzo de 2002. La lista de miembros de 29A es cada vez más pequeña. Se han ido Mandragore y Lord Julus, por *"discrepancias con el grupo"*[87]. También se van Tcp y Super. Vuelve Z0MBiE y se une a ellos Ratter. Forman el staff 6 personas.[88]

A pesar de que este número llega repleto de buenos artículos (25), herramientas (19) y virus (43), lo que llama la atención son tres textos, escritos por VirusBuster, Benny y Z0MBiE, sobre la decadencia de la escena vírica. VirusBuster justifica así que han tardado más de un año en sacar nuevo número:

> He estado en la escena VX muchos años y no recuerdo una situación tan mala, y no es fácil entender cómo hemos llegado a esta situación, posiblemente porque las razones son múltiples. La mayor causa de esta situación es que han abandonado la escena algunos de los mejores programadores de virus: Jack Qwerty, b0z0, Bumblebee, etc., pero el problema real es que no hay nuevos programadores que reemplacen a esos monstruos.[89]

En una entrevista que le hace el diario El País, VirusBuster afirma que la escena vírica está muriendo:

> VB-De los veinte o treinta escritores de virus de alto nivel que existían hace cinco años, se ha pasado a menos de diez. Quedan pocos escritores de virus que sean capaces de sorprender y hacer cosas originales.
> MM-Pero si esto está más lleno de virus que nunca...
> -Pero virus de baja calidad, hechos por gente que no pertenece a la vx scene.
> -¿La escena se ha hecho vieja?

-La media ha pasado de los 20 a casi los 30 años.
-¿Sólo quedáis vosotros a nivel mundial?
-También está IKX, pero están pasando por una crisis de la que les será difícil salir.
-Os debéis sentir muy solos…
-El sentimiento es de que ya no queda mucha gente que lea nuestra revista y entienda todo lo que se explica.**[90]**

Benny se queja de lo mismo:

> La escena y muchas cosas en ella no volverán a ser como antes. Algunos programadores hablan de "muerte", "decadencia", algunos hablan de serios problemas. (…) Los script kiddies y sus llamados "virus/gusanos" mandan en el cibermundo. (…) Los antivirus ganan dinero de gente cuya estupidez es, en un 99,99%, responsable de grandes epidemias víricas (tipo los gusanos "pincha-aquí"). ¿Dónde están aquellos programadores de élite, grupos de élite? ¿Dónde están aquellos virus de alta tecnología que *ayer* dominaba el mundo? *Decadencia*.**[91]**

La escena se ha hecho vieja, explica Benny, los lenguajes de alto nivel dificultan el acceso a los novatos, y crear virus está prohibido. Desde hace un par de años cuerpos policiales de todo el mundo ha empezado a detener a creadores de virus, responsables de infecciones masivas, como Win95.CIH o Melissa, algo que ha ayudado a criminalizar (más) a la escena vírica.

Pero es Z0MBiE quien, en este sexto número de 29A, escribe la esquela más bella:

> Hacer virus está muriendo. Además, este proceso está a punto de llegar a su punto de no retorno. Lo vemos en el número cada vez más pequeño de ezines al año, de grupos llenos de miembros zombi, en que ya no se producen nuevas tecnologías víricas, en el decreciente número de virus para Win32, en las toneladas de script virus, que son todos iguales, y en el nulo interés por desarrollar virus, a nivel mundial. Es aún más triste porque muchos de nuestros esfuerzos y nuestro tiempo y nuestro poder y nuestras vidas se gastaron para crear todo esto. Paredes de la casa que contruimos se están cayendo. La única forma de hacer que este proceso sea reversible es unirnos, usar nuestro conocimiento, nuestro poder y nuestra fama y nicks para interesar a gente nueva, resistir un poco más y empezarlo todo de nuevo, antes de que sea demasiado tarde.**[92]**

3.3.7. Issue # 7/La criminalización y la asimilación en la industria

Dos años después, en febrero de 2004, aparece el séptimo número de 29A. Benny anuncia que se va del grupo, pues ha encontrado un trabajo que le gusta y le queda poco tiempo para hacer virus: *"Aquellos tiempos adolescentes, cuando podía sentarme ante la pantalla todo el fin de semana, se han ido. La vida es algo más que eso"*.**[93]**

En sus últimas palabras, Benny se queja una vez más de la muerte de la escena vírica, donde hay *"más gente interesada en diseminar y hacer daño que en la programación de material vírico técnicamente avanzado"*. Denuncia también que un viejo ex-compañero de 29A, Darkman, le ha echado del canal #virus de Undernet porque su nombre apareció en un artículo del "New York Times".**[94]**

Y es que Benny se ha hecho famoso. Tanto que, en noviembre de 2004, cuando lo contrata una compañía checa, Zoner Software, cuyo producto estrella es el

antivirus Zoner, se monta un pequeño escándalo[95] porque, según algunos, transmite el mensaje de que escribir virus sirve para encontrar trabajo. Zoner Software alega que confía en Benny porque tiene una gran ética y Benny se defiende en una entrevista con "CNET News":

> Un montón de buenos escritores de virus hoy trabajan en la industria de antivirus. No quiero causar problemas a mis amigos, por lo que no daré ejemplos concretos. ¿Quién más podría escribir programas antivirus? ¿Quién más tiene la experiencia y las habilidades técnicas para luchar contra los virus? Casi todos los ex-miembros y actuales miembros de 29A están trabajando en la industria de los antivirus y la seguridad informática.[96]

Semanas después, en diciembre de 2004, la policía checa lo arrestará como sospechoso de crear el gusano Slammer[97], aunque jamás se encontrarán pruebas.[98] [99]

Anuncian también su marcha de 29A Mental Driller y Super. Vuelve Vecna y roy g biv se une al grupo. Ahora son 7.

La revista sigue fiel a su calidad y mucha información: 32 artículos, 27 herramientas y 47 virus, entre ellos una muestra del gusano MyDoom, que en enero de 2004 se ha convertido en el gusano de correo electrónico que se ha diseminado más rápido.[100]

Pero, a pesar de seguir teniendo mucho material, la revista transmite una sensación de vacío y depresión. 29A lleva 8 años en activo, algo muy poco común en los grupos de hackers. Es el último Mohicano, viejo y agotado, de una escena vírica que agoniza, un barco a la deriva en un mar muerto, con una tripulación borracha de decadencia, que gasta sus últimas energías en disputas internas.

La sección de Noticias de la ezine muestra el árido contexto en el que 29A sigue tratando de estar vivo, último dinosaurio de una era que termina: en los últimos dos años, explica VirusBuster, casi no ha habido noticias en la escena vírica[101]. Se han anunciado nuevos grupos y revistas que jamás aparecieron, el conocido foro Vx Heavens ha cerrado y el sitio coderz.net se recupera de un largo ataque.

> Durante estos dos años la producción de macrovirus y virus en general ha disminuido mucho. Actualmente los programas antivirus están más enfocados a desarrollar "suites" de seguridad (anti-spam, cortafuegos, etc) que programar nuevas técnicas antivirus. Más de la mitad del material que se añade a las bases de datos de detección es código maligno: puertas traseras, troyanos, exploits, etc.[102]

Y el golpe de gracia: los creadores de virus ya no son artistas, son criminales peligrosos por los que se ofrecen recompensas, como en el salvaje Oeste.

> Microsoft ha destinado 5 millones de dólares para pagar recompensas a quien dé información que lleve al arresto y prisión de los programadores de virus. Se han ofrecido recompensas por los autores de Blaster, mydoom o Sobig.[103]

David L. Smith, autor del virus Melissa[104], ha sido sentenciado a 20 meses de cárcel; Simon Vallor, a dos años por diseminar los virus Gokar, Redesi y Admirer.[105]

El colofón es la detención de la programadora de virus belga Gigabyte[106][107], buena amiga de 29A y personaje muy conocido en la escena vírica[108]. Las autoridades belgas detienen a la joven en su casa el 9 de febrero de 2004, justo unos días antes de la publicación del séptimo número de 29A.

Gigabyte se enfrenta a una posible condena de 3 años de prisión por daños informáticos. Finalmente todo quedará en nada pero la fuerza simbólica de su detención es un hachazo para la escena. Junto con Gibabyte, caerá el sitio coderz.net para no volver jamás. Tampoco a Gigabyte se la volverá a ver en los canales habituales de chat. Al menos no con este nickname.

3.3.8. Issue # 8/Morir creando

El 1 de enero de 2005 aparece el último número de la revista. Su nueva web es http://vx.org.ua/29a/ que se mantendrá hasta la actualidad (12-12). Además, por fin el grupo tendrá su propio dominio: 29a.net. Whale y dis69 (también conocido como Lord Yup), que se unieron a 29A en marzo de 2004, lo han abandonado en noviembre. Ratter también se ha ido. Vallez entró en mayo y con él ahora son 6 miembros: GriYo, roy g biv, Vallez, Vecna, VirusBuster y Z0MBiE.

En un último alarde de gloria, el grupo presenta al mundo el primer virus que infecta plataformas Win64 (**Rugrat**, obra de roy g biv), el primero que infecta PDAs (**Dust**, hecho por Ratter) y el primer virus que ataca teléfonos móviles (**Cabir**, creación de Vallez). 21 artículos, 20 herramientas y 26 virus llenan la última revista del último grupo de creadores de virus de élite.

El texto de introducción a este octavo número es una defensa de los creadores de virus ante la criminalización rampante y una declaración de intenciones:

> Entonces, ¿diseminar sí o no? La respuesta parece obvia. La diversión está en la creación y los problemas en la propagación.[109]

Esta declaración se enmarca en una reciente sentencia contra un ex-miembro del grupo, Whale, quien tendrá el dudoso honor de ser el único integrante de 29A condenado por las autoridades de su país: en noviembre de 2004, un juez ruso lo considera culpable de crear los virus *Stepan* y *Gastropod* y *"publicar su código, así como el código fuente necesario para crear nuevas variantes en diversas webs underground de intercambio de virus. Se le consideró culpable y condenado a pagar 3.000 rublas (105$)"*.[110]

3.4. El fin de 29A

A partir de enero de 2005, cuando aparece el octavo número de la ezine, el silencio inunda la web de 29A... Hasta enero de 2007, cuando una nota informa que GriYo, Vecna y Z0MBiE se van, mientras el resto del grupo (roy g biv, ValleZ y VirusBuster) asegura estar *"intentando decidir el futuro de 29A"*. En julio, otra nota dice que no saldrán más números de la ezine y que se creará un foro. En diciembre, The Register explica que roy g biv ha abandonado 29A y hace al menos un año que

nada se sabe de ValleZ.[111]

Por último, el 26 de febrero de 2008, VirusBuster escribe la esquela de 29A:

> +He intentado contactar con ValleZ para tomar juntos una decisión sobre el futuro de 29A, pero no he tenido suerte, por tanto he decidido tomar esta decisión solo. Y mi decisión es que 29A está oficialmente retirado. Me siento legitimado ya que soy una especie de alfa y omega del grupo. 29A nació en Dark Node, mi BBS, y soy el último miembro activo del grupo. Mis últimas palabras como miembro de 29A son para toda la gente que trabajó duro para hacer que este grupo fuese el mejor: Muchas gracias! Hasta la vista, VirusBuster/29A.
>
> +29A ha abandonado el edificio![112]

Años después, en una entrevista[113], ValleZ explicó su visión del por qué murió 29A y la causa de su silencio cuando VirusBuster lo buscó para finiquitar el grupo:

> -¿Qué acabó con 29A?
> -Creo que la falta de contribuciones por parte de los miembros que ya había y la falta de nuevos miembros es la raíz del problema. Algunos miembros simplemente no contribuían ya, o apenas nada. Otros tuvieron que dejar el grupo por cosas legales en su país, como Whale,Ratter y Z0mbie creo. A eso se sumaron problemas internos entre algunos miembros del grupo. En mi caso personalmente me vi en mitad de la "batalla" entre dos de los miembros, dos personas a las que respeto, y esa fue una de las razones por las que me aparté bastante del tema. Además, aunque tenía dos virus para contribuir para la #9, llevo ya como dos años sin codear nada. Roy G Biv es el que más se lo curró hasta el final, pero imagino que viendo la progresiva desintegración del grupo decidió abandonarlo. Creo que empezó a publicar en otro grupo.[114]

En los comentarios a esta entrevista, en el blog 48bits, se desató una batalla verbal entre GriYo y VirusBuster, que mostraron en público, por si había dudas, la mala relación entre ambos.

La muerte de 29A fue un acontecimiento de alcance mundial. El periodista John Leyden daba su interpretación de los hechos en "The Register":

> La muerte de conocidos grupos VX es una muestra del desarrollo sintomático de cambios en el mercado del código malicioso. El beneficio económico ha reemplazado a la travesura, la curiosidad intelectual o el deseo de hacerse famoso creando virus. Los escritores de virus tradicionales se han ido de la escena para ser reemplazados por programadores más oscuros que crean troyanos sofisticados destinados a generar beneficios ilícitos. La persecución policial contra los escritores de virus ha actuado como desincentivo sólo para los "hobbistas".
>
> Ahora, además de las pruebas de concepto de código malicioso al estilo de 29A, tenemos que lidiar con troyanos y otros sofisticados clientes de botnets "desarrollados por profesionales". Los días del "malware" que borraba música gitana rumana, hablaba con sus víctimas o creaba un juego, que permitía a los usuarios de ordenadores infectados tirar cocos al experto en antivirus Graham Cluley, se han convertido en reliquias de otra era.[115]

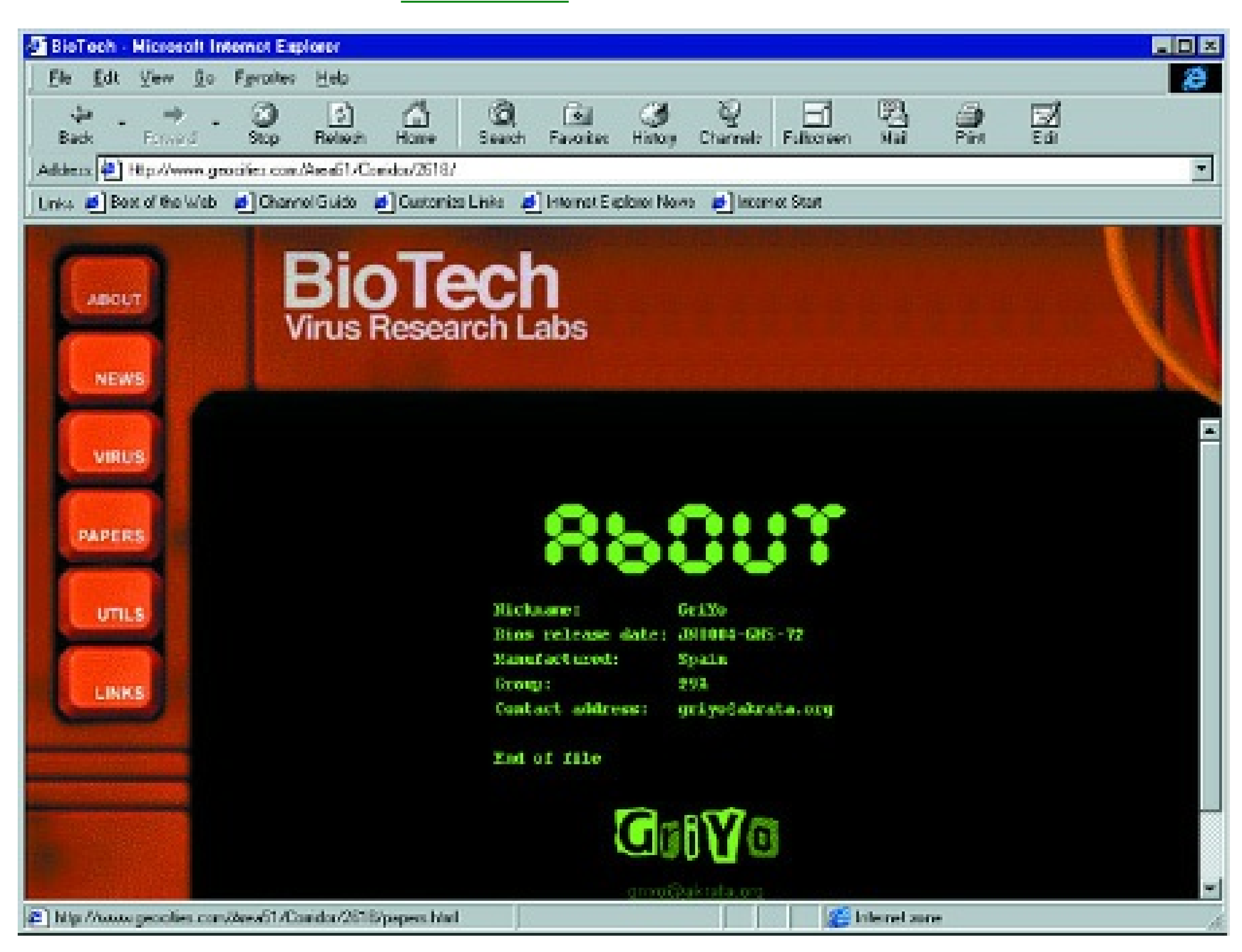
3.5. Virus destacados

La producción de la factoría 29A fue tan impresionante, en cuanto a calidad y calidad, que es difícil destacar unos pocos virus.

Vida en Saturno. En el primer número de la ezine, Mister Sandman anunciaba que iba a mandar un virus a Titán, una de las lunas de Saturno:

> No, no estoy borracho: en octubre de 1997 la sonda Huygens, un proyecto de diversos países europeos, aterrizará en Titán, la luna més grande de Saturno, para buscar indicios de vida, Dentro de esta sonda habrá un CD en el que la gente, a partir de dentro de unos pocos días, podrá escribir su nombre y el texto que quieran. Y como el espacio para escribir este texto es suficientemente grande como para contener un virus, he decidido mandar uno, por tanto será el primer virus del mundo que llega a otro planeta.**[116]**

AntiETA. GriYo creó este ejemplar de laboratorio como protesta por el asesinato de Miguel Ángel Blanco. Quien se infectaba veía en su pantalla una imagen de una mano blanca. Era un virus hacktivista.



Después de su marcha de 29A, GriYo creó una web propia

Marburg. Obra de GriYo. Fue el primer virus polimórfico de 32 bits. Se propagó por el mundo a gran velocidad, debido a que las revistas “PCGamer” y “PC Power Play” regalaron CDs que contenían programas infectados con este virus. También el CD del juego MGM/Wargames salió al mercado infectado.

Marbug se entiende mejor puesto en contexto: en octubre de 1997, GriYo acababa de crearlo y comprobó que ningún antivirus existente en el mercado podía detectarlo. Diversos miembros de 29A estaban aquellos días enfrascados en discusiones con personas de la industria antivirus, en el grupo de noticias alt.comp.virus. 29A les criticaba que hacían publicidad engañosa, ya que sus

productos no detectaban el 100% de los virus. La respuesta de la industria fue burlarse del grupo.

Entonces, en noviembre de 1997, aparece Marburg y debido a su complejidad ningún antivirus será capaz de detectarlo hasta nueve meses después, cuando ha tenido tiempo de infectar miles de ordenadores.

HPS, también creado por GriYo, es el primer virus polimórfico para Windows98. Lo curioso es que aparece antes que se lance al mercado este sistema operativo. Más adelante pasará lo mismo con Windows 2000 : Benny y Darkman crean **Win2000.Installer**, cuando Windows 2000 aún no se ha presentado oficialmente.

Tuareg, de The Mental Driller, cambiaba la página de inicio de Netscape y Explorer por el Sitio del Hambre http://www.thehungersite.com, y hacía que, cada vez que se abría el navegador, se pinchara en un espacio de la web donde se daba dinero al Tercer Mundo. Otro virus activista de Mental Driller fue **MetaPHOR**, que cada 14 de mayo, día de la proclamación de Israel como estado independiente, activaba el mensaje *"Free Palestine!"* (Palestina Libre) en los ordenadores infectados que tuviesen activado el lenguaje hebreo.

3.6. Ética

La creación de virus en 29A no buscaba un fin destructivo sino creativo, de aprendizaje, reto intelectual y fascinación por la vida artificial. La ezine siempre se acompañó de un texto donde el grupo trasladaba este espíritu:

> Se supone que muchos de nuestros lectores tienen más de un virus y son incluso capaces de crearlos por ellos mismos, por lo que no son los típicos lamers que están buscando código destructivo para joder los ordenadores de su escuela (...). Tenemos una norma interna que prohibe incluir cualquier código destructivo en nuestra revista. Preferimos apostar por la originalidad y escribir código por diversión, para que nuestros virus puedan ser útiles para la gente que está aprendiendo.**[117]**

En el tercer número, se adoptó para siempre un texto estándar, que añadía:

> Escribimos virus por diversión, porque es nuestro "hobby", no porque queramos hacer daño a la gente o meternos en problemas. Escribimos virus para inventar nuevas técnicas, mejorar las existentes y aprender más sobre los diversos sistemas operativos. Sabemos que hay cientos de otras formas de hacer esto, probablemente mejores, pero esta es la que nos gusta.**[118]**

4. H/P/A/V/CRACKING: Karpoff y Whiskey Kon Tekila

La escena del cracking evoluciona mucho en los años 90. Claudio Hernández, murciano, experto en carding (manipular tarjetas bancarias, telefónicas, de TV, etc.) y cracking, escribe 5 libros entre 1994 y 2000. Es la edad de oro del cracking de tarjetas de televisión de pago y Hernández tiene abundante información:

> Todo empezó allá por el año 89 descodificando los sistemas de video y audio analógicos de los pocos canales que existían. No fue hasta el año 2000 que se abrió la tarjeta de acceso condicional de Vía Digital y Canal Satélite. Existieron muchos hackers en aquella época dorada y cada uno resaltó en lo suyo, desde descifrado de algoritmos hasta el desarrollo de hardware para programar las tarjetas o emularlas.**[119]**
>
> He conocido de primera mano a los que han clonado con éxito las tarjetas inteligentes de los principales canales de pago y al mayor cracker de Europa, que fue detenido no porque había roto todo los sistemas de cifrado de televisión sino porque empezó a fabricar y comercializar decodificadores piratas".**[120]**

Cuando no escribe libros, Hernández es un cracker con el nick **OverrideSidek**. Está especializado en *hardware cracking*, que significa romper el sistema anticopia de Macrovisión o sistemas de lectura de tarjetas. Pero no todo sirve para ver televisión: también se emulan tarjetas bancarias y de cabinas telefónicas, de banda magnética. Después vendrán las que llevan EEPROM y las de chip.

Pero, a excepción de Hernández y sus libros, esta escena cracker, tan grande como la parte no visible de un iceberg, es muy reticente a salir a la luz, pues se juega el ir directa a prisión.

> El carding movió en España miles de millones de pesetas, sobre todo en las tiendas de electrónica. Se descubrieron decenas de hackers y crackers muy buenos con una magnífica capacidad para jugar con algoritmos RSA y otros. Era la época también de las tarjetas emuladoras de teléfonica. Se crackeó incluso la de los teléfonos móviles.
>
> Se cambió el curso de Via Digital y Canal Satélite Digital. Hubo detenciones, traiciones, odios, envidia. Las empresas del sector del satélite financiaban la elaboración de emuladores piratas, la colaboración llegó hasta China, Corea del Sur y Japón además de toda Europa. Fue todo un mundo mágico y lleno de sorpresas.
>
> Es una época dividida en dos fases, que duraron cada una diez años. La primera, la del hardware-cracking, la cuento en mis libros, pero la segunda, la del hacking, es más peligrosa y creo que se quedará en mis recuerdos... me da miedo escribir algo por las represalias.**[121]**

A finales de los 90 se darán a conocer otros grupos y proyectos sin ánimo de lucro, relacionados con el cracking y la ingeniería inversa. Son la parte visible y menos delictiva del iceberg del warez. Su nodo principal es una magna biblioteca en línea de manuales, herramientas y traducciones, aportadas por el ingente esfuerzo de la comunidad cracker, llamada **Karpoff Spanish Tutor** o **La página de Karpoff**.

5. La página de Karpoff

En sus tres años y medio de existencia, la página de Karpoff recopiló 558 manuales y cursos, un centenar de traducciones, un centenar de crackmes y otro centenar de herramientas, todos creados por la comunidad hispana interesada en cracking, ingeniería inversa y programación informática. El sitio contaba también con foros, una lista de correo donde se informaba de las actualizaciones y multitud de enlaces. Era el "hub" de esta comunidad en lengua castellana.

> Muchos de vosotros ni os imagináis que hace unos 4 años no habia apenas manuales en español sobre cracking, y a dia de hoy estamos sobrados de informacion.**[122]**



La Página de Karpoff se puso en marcha el 30 de julio de 1999 y la última actualización es de 18 de enero de 2003. No tenía una dirección fija. Las principales redirecciones que permitían localizarla eran: http://come.to/karpoff, http://go.to/karpoff y http://welcome.to/karpoff . Siguen activas en el momento de escribir estas líneas (enero de 2013) y apuntan todas al mismo sitio web: http://mirrorkarpoffespanishtutor.comxa.com. Existe otra web prácticamente idéntica, un espejo, http://karpoff.galeon.com, que dejó de actualizarse en 2002.

Karpoff Spanish Tutor contaba con una activa comunidad. Tenían especial éxito las compilaciones de cursos y manuales, como los *Tutoriales Crack* que hacía **Profesor_X**. La Página de Karpoff albergaba también proyectos colectivos de traducción, como las *Cracker Notes de Tornado en español*, que lideró **Txeli**, y otros. Cabe aclarar que a día de hoy es difícil consultar la mayoría de cursos y herramientas guardados en la web, ya que precisan contraseña para acceder a ellos.

5.1. Quién fue quién: el core

Hay poca información sobre el creador de este sitio, **Karpoff**. Parece que empezó en solitario la aventura, el 30 de julio de 1999. Algunos mensajes del *Registro de Actualizaciones* de la web reflejan que vivía en Donostia y era estudiante**[123]**.

Karpoff escribía cada semana al menos un mensaje, que se guardaba en el *Registro de Actualizaciones*. Gracias a este archivo es posible reconstruir la historia del sitio. Los textos más antiguos están fechados en octubre-noviembre de 1999 y son notas escuetas de nuevos manuales o secciones. En julio del 2000 un mensaje anuncia el "Primer Aniversario de esta página":

> Si me permitis hacer una valoracion creo que es muy positiva, entre todos hemos conseguido reunir una gran cantidad de documentos en castellano y lo mas importante son proyectos propios de nuestra cosecha. Gracias a Todos.**[124]**

El 2 de octubre del 2000, otro mensaje de actualización muestra que el sitio

funciona a toda vela:

> Ha sido tal la cantidad de material recibido en este año que me veo obligado a hacer algunos cambios para agilizar la carga de la pagina[125]

También se anuncia la puesta en marcha de una nueva sección, sobre desprotección de juegos, que llevará **Gadix** (más adelante **Mr. Ocean**, miembro de WkT!). Días después, a finales de octubre, Karpoff detalla los nombres de los primeros colaboradores del sitio: **Godrigo2k**, **BacteriOO**, **Keko**, **Nandois**, **Perico**, **^[Trodi]^**, **Ruben**, **Jon_rat** y **Troba.**[126]

No aparecen nuevos colaboradores hasta abril de 2002, cuando Karpoff pide públicamente ayuda para montar una sección de hacking y **Xirtam** acude a su llamada. Por último, llega **Ojad**, quien se unió como webmaster a finales de 2002.[127]

5.2. Quién fue quién: la comunidad

El esfuerzo vertido en la Página de Karpoff tuvo una consecuencia que posiblemente en aquel momento no se previó: cada manual o curso se presentaba con el nombre de su autor, de forma que su recopilación permite hacerse una idea de quién era quién en la escena cracker hispana de finales de los 90 y principios del 2000.

> **Ricardo Narvaja** 20/02/2001: Curso de Cracking para Newbies (Es un curso con muchos capitulos y con ejercicios, se mantiene a traves de una cuenta de correo en plan foro, su autor va tratando todo tipo de temas y el nivel del curso va subiendo)[128]

De aquellos creadores, traductores y recopiladores de documentos y programas destacan, por la cantidad y calidad de sus aportaciones, **Profesor_X**, **Dek_Oin**, **Act_Mag0**, **Andrik**, **Arkamian**, **nuMIT_or**, **Demian**, **CaoS ReptantE**, **Marmota**, **Crack el Destripador**, **Txeli**, **Muñoz**, **KuaTo_ThoR**, **X-Grimator**, **Ricardo Narvaja**, **JoTaKe**, **JaruNet**, **Maniac PC (KarlitoxZ)**, **Fanega**, **FranTic**. También: **Gerza**, **D.A**, **Mr.Blue**, **Nio**, **PicsOne**, **MeGaBiTe**, **John Keeper**, **Deejay Mihai**, **SV**, **Sable**, **Pablo Barron**, **Vinshuka**, **Black Fenix**, **Txabo**, **Lecter**, **Migmas**, **SiLvEr StOrM**, **noseman**, **Relay**, **Makkakko**, **NickyAC**, **LEiRUS**, **ViPER**, **Metamorfer**, **Skuater**, **AusPex**, **Mr. Burns**, **RAZiEL**, **Stomper**, **Xaxs**, **Para**, **D14bl0**, **Esiel2**, **Espawn**, **Sinmoneys**, **Villano bAjo**, **Yerba Mate**, **Kamui**, **+Er@ser**, **CaR19**, **Loko2000**, **Crkvlugo**, **Cap_kirk69**, **SiLvEr StOrM**, **zerU**, **^DeStRoY^**, **Toroborracho**, **Aftosa**, **Corinto**, **Mnemox**, **Stavros**, **Willy Walker**, **Oscar Maza**, **!!!JNP**, **Good cracks**, **Charlie**, **Gohan**, **Snacker**, **MrCrimson**, **Izelon**, **R!SC**, **Alexis Rojas**, **Txotxo**, **Storm**, **Sinmoneys**, **crick**, **MaGuNa teAM**, **xzErO_**, **KEENER**, **Roberto Reategui**, **MGN**, **El Alfil**, **Juan**, **Maximodutty**, **Dark Cracker**, **^[G]oLe[E]^**, **Eliecer**, **Klaudius**, **ckener**, **MacCPP**, **VirCor**, **Loco**, **Armando**, **Orlando**, **Carlos**, **boocrax**, **Cesar**, **wilches**, **Chechon**, **ElRengo**, **Mr.White**, **AlamBike**, **BYtEsKrAcK**, **Gezz**, **GAMESPACK**, **Jack**, **El Pollo**, **Calculici**, **sNoOfy**, **Makelolo** , **§mÂ$|-| & !<@ßØ0m**, **Guitar Freak**, **YaNtIpArZi**, **Pedrolas**, **BiRKiN**, **iDznaK**, **CbtO**, **DeAtH**, **cap_kirk69**, **Nopper**, **Mr.Floppy**, **Snop**, **Riverwind**, **rulzgz**, **Sorvats**, **David Penalva**, **KhaNeTe**, **Leoz**, **OGRY**, **Lutino**, **Rul**, **crkvlugo**, **3d0$**, **Mr. Ridk**, **Keops**, **Fantomas**, **Migmas**, **Cronos**, **LiuTaoTao**,

ZhuNanHao, **Mr Silver** (antes **Black Fenix**), **Mr Snow** (antes **Skuater**), **Strom**, **V0LtI0**, **CKENER**, **ByTESCRK**, **Pepote**, **^DeStRoY^**, **Kidd**, **Saccopharynx**, **VisionZ**, **El Cuervo**, **The Pope**, **Ciriaco Garcia**, **Hutch**, **Marconi**, **uNO mAS**, **WSEXM**, **Asterion**, **Tamoxifeno**, **@GZRiP**, **Francisco**, **Juan**, **NI2**, **Angus Johnson**, **Nacho Cabanes**, **Mario Gonzalez**, **Leonardo Javier**, **SoTaNeZ**, **LeafaR GV**, **Mongui**, **Arkanian**, **X**, **DGrojo**, **MacEdu**, **[Moneo]**, **Cubafreak**, **BugSys**, **Crkviz**, **balitog**, **KlimaX**, **WiShMakEr**, **Alpine**, **Yado**, **ACiD BuRN**, **MaV3RiCk**, **GrandPa**, **+Tsehp**, **Renegade**, **Sujeto Tacito**, **Shark**, **Eternal_Bliss**, **joined**, **Snake**, **TurboP**, **AntiXryst**, **TC**.

En cuanto a grupos de cracking, se menciona repetidamente a **K-For**, Whiskey Kon Tekila, TNT!Crack!Team, **MaGuNa teAM**, **Kr@cKerZ United Team (KUT)**, Askatasuna Krackers Society y la lista CracksLatinos, administrada por Ricardo Narvaja.

Por otra parte, la sección de enlaces de La Página de Karpoff nos permite hacernos una idea de otros puertos donde se refugiaba la comunidad cracker hispana, como **Demian Site (TNT)**, **La Pagina de KarlitoxZ**, **Mr.Crimson Web SiTe (WkT!)**, **The PoPe**, **DuxAs Site**, Stomper Site, **Reversed Minds** (by Black Fenix), **Txeli Site**, **Hackers Dark City Mexico (by Dark City)**, **La Peich del Flaco**, **Mr_Burns Site**, **Totxo_Site**, CRAAAACK (by Crack el Destripador & Marmota), **Provided minds**, **X-Faktor Site**, **Unevil's Site**, **Mr.Ridk Web Page**, **Rul Cracking Web**, **Software Security against Piracy** (by NI2), **La taberna de Mou**, **La página de Mefhigoseth**, **nuMIT_or's Programming Page (KUT)**, **La Página De Nacho Cabanes**. Sin olvidar, a nivel internacional, las grandes islas: **Neworder**, **Astalavista** y Fravia's mirror of Reverse code engineering.

5.3. Problemas de hosting

La Página de Karpoff cambió diversas veces de alojamiento, siempre en sitios gratuitos o servidores de simpatizantes. Cuanto más éxito tenía, las visitas y descargas la saturaban y obligaban a buscar un nuevo hosting, de lo que se quejaba regularmente Karpoff:

> Hola Señor@s !!, Mantener las compilaciones en linea es un infierno (como ya os habréis dado cuenta), cifras en estas 2 semanas se han hecho aproximadamente unas 8.000 o 9.000 descargas de las compilaciones de Tutoriales Crack 2000-2001 , si son muchisimas, hay el problema para mantenerlas en un servidor sin que te lo borren por exceso de descargas.**[129]**

Un problema añadido era la temática del sitio, el cracking, que muchos alojadores gratuitos no aceptaban:

> Cada vez es mas dificil mantener la pagina operativa, los server botan la pagina a la de dos dias, por eso me es imposible asegurar que la pagina funcione medianamente bien, aprovechandome de vuestra buena voluntad os pregunto, alguien tiene un server seguro donde poder alojar la pagina ??? , como podeis observar no hay cosas ilegales, no hay cracks, ni warez, ni porno, ni esas cosas por lo cual borran las paginas, pero solo por estar dedicada a la ingenieria inversa esta en la lista negra de todos los servidores.**[130]**

Cabe decir que la mayoría de páginas de cracking vivían los mismos vaivenes, como explica Gerza en sus *FAQ sobre ingeniería inversa*. La diferencia es que la web de

Karpoff duró bastante más que la mayoría.

> Las web de crk suelen tener una vida corta y dinámica (a excepción de fravia). Lo cual quiere decir que los enlaces aparecen y desaparecen, y los contenidos varían con cierta asiduidad.**[131]**

5.4. Página cerrada

Una actualización fechada el 12 de enero de 2003 anuncia: “Karpoff Cierra la Pagina”**[132]**. No es una sorpresa pues más de una vez en los últimos años se ha quejado del trabajazo que le da la página:

> Ufff necesito decirlo, sabeis cuanto me ha llevado actualizar la pagina ??? nada mas y nada menos que 15 HORAS (siempre que actualizo la pagina mas o menos las mismas horas) buaa sniff, ya no tengo tiempo ni para crackear snifff, hace que no cojo el sice, meses, por favor, podéis ayudar??, solo con enviar los manuales en la plantilla es un gran adelanto, (…) es que no vivo mas que para mantener la pagina, (…) tener piedaddddd de mi almaaa :)**[133]**

En 2009, Karpoff reaparece en un foro y explica las causas objetivas que le llevaron a cerrar la página:

> El trabajo no me permitió seguir con la pagina e hice todo lo posible para que otras personas se hiciesen cargo del proyecto, pero no lo conseguí.**[134]**

5.5. La memoria de X-Grimator

En 2008, un post en el blog 48Bits resucitaba la memoria de la comunidad de crackers que pululó por La Página de Karpoff. X-Grimator escribió en los comentarios una emotiva glosa de aquella aventura:

> Recuerdo mucho aquella época de inicio de la Ingeniería Inversa. Recuerdo mucho a aquel grupo de curiosos con sed de aprender que nos ayudábamos desinteresadamente unos a otros. Recuerdo mucho aquella frescura, aquel afán de saberlo todo.
>
> Para mí fue una familia virtual, los primeros contactos importantes con la informática (no olvidéis que yo soy abogado), el equipo Whisky kon Tekila, Windows 95, las primeras distros de Red Hat…
>
> No olvidaré jamás en mi vida el canal #crackers, de ese IRC-Hispano que agoniza, ni las bromas el Día de los Santos Inocentes donde siempre “detenían” a alguno de nosotros. Nunca olvidaré el día de Navidad cuando supimos que nuestro querido esn_mIn había muerto y que tan apenados nos dejó.
>
> Queríamos saberlo todo, queríamos (sin ninguna maldad ni daño a nadie) crackearlo todo. El Pope, Craaaacker, numit_Or, TKA, Spark, Mr Black, Mr White… Wendigo, los foros de Wkt, los de Viva el Jamón y el Vino, las conexiones a 56k…
>
> Todos esos recuerdos se desvanecerán como lágrimas en la lluvia.
>
> Recuerdo a mi familia cracker con mucha intensidad, algo lejanos en el tiempo, pero con mucho cariño. Estaba ansioso por llegar a casa y chatear con ellos, por resolver esa protección de una vez, por nopear algo. Ellos asentaron unas bases importantes en la informática actual. Fueron los primeros gracias a los cuales pudimos tener un Winzip gratis y

cómodo, un juego copiado para un amigo, un Office con número de serie.

> Para mí es un honor del que estoy muy orgulloso haber sido una pieza pequeñita en ese puzzle, un componente más de ese conjunto de locos sedientos de conocimientos que, sin ayuda de nadie, llegaron a escribir toneladas de información libre para todo el que quisiese saber algo más en su vida.
>
> A ellos, a esa época, dedico mi recuerdo con la cabeza bien alta de haber sido un cracker.
>
> X-Grimator**[135]**

5.6. Whiskey kon Tekila!

El grupo más importante de la comunidad cracker hispana es sin duda Whiskey kon Tekila! ([WkT!]), que nace en 1997, de la mano de **Mr.WhiTe**, a quien algunos creen oriundo de Asturias. La versión en inglés de la web es el único vestigio que se conserva: Whiskey Kon Tekila -=The Original Spanish Reversers=-. El grupo muere en 2001.



WkT! logró reconocimiento internacional**[136]** y en La Página de Karpoff se hablaba de ellos con mucho respeto:

> http://wkt.mypage.org (LA referencia)**[137]**

Uno de sus miembros, Mr.Snow, confirma que eran El Grupo:

> Yo siempre quise formar parte de ese grupo ya que en aquellos entonces eran la elite y todos querian pasar por el.**[138]**

Sus medios de comunicación eran un sitio web, una lista de correo interna creada en 1999**[139]** que duró hasta 2002 y un canal de chat en EFnet, *#wkt*. También solían andar por el canal *#crackers* de IRC-Hispano. Mantenían un foro web de gran renombre, que desapareció en 2001.**[140]**

> Por entonces había un foro de cracking genial (el WKT) al que accedía desde la page de Karpoff, que de pronto chaparon y nos quedamos a dos velas.**[141]**

5.6.1. Miembros

Los primeros integrantes del grupo, en 1998, eran Mr.WhiTe, **Mr.Black**, **Mr.Purple**,

Mr.Red, **Mr.Pink**, **+Aitor** y **JUANDA**. **ESTADO+PORCINO** no formaba oficialmente parte del grupo pero estaba muy cerca.



Sus *nicks* eran colores debido a la influencia de la película Reservoir Dogs, que encantó al fundador, Mr. White.

En 1999, fecha de la última actualización de la web en inglés[142], se habían unido al grupo **Mr.Brown**, **Mr.Crimson**, **Yeyo**, **Mr.Green**, **Mr.Grey**, **Mr.Orange**, **Mr.Blue** y **Mr.Cyan**. En cuanto a Mr.Purple y Mr.Red, debían haberlo abandonado y aparecían en la *Hall of Fame*[143]. Más adelante entrarían **Mr.Ocean**, **Mr.Snow**, **Mr.Jade**, **Mr.Yellow**, **Mr.Silver** y **Mr. Mauve** (antes Karlitox).

5.6.2. La pasión por dar información

El grupo explicaba en sus FAQ -iniciadas por Mr.Red en 1997- que lo movía su interés por liberar información sobre cracking:

> Desde sus orígenes, el objetivo de Whiskey Kon Tekila ha sido, es y será siempre proporcionar información. Por diversos motivos (principalmente económicos) la Ingeniería Inversa siempre se ha considerado un tema "tabú" en la Informática. Y como tal, el desconocimiento técnico en este sentido ha sido notable. (Al menos en el mundo hispano hablante). [WkT!] surge como un grupo de gente apasionada por la programación de protecciones hardware/software, con el único propósito de ampliar su conocimiento y el de cualquier otra persona interesada al respecto. [144]

Más concretamente, el objetivo era formar a los programadores mostrándoles cómo se desprotegían sus programas en "el otro lado":

> Los programadores de aplicaciones comerciales suelen actuar con una cierta indiferencia cuando se trata de programar la protección de su software. (...) Desconocimiento, en definitiva, de las técnicas empleadas desde "el otro lado". Es por esto que estas páginas constituyen (o eso se pretende) un punto de referencia para todo aquel programador realmente interesado en ampliar sus conocimientos y adaptarlos a los nuevos tiempos.[145]

Algunos integrantes de WKT destacaron en la creación de herramientas para el cracking, como Mr.Crimson y su *TOPO*. Algunas herramientas de WkT se ofrecían en La Página de Karpoff, como *WKT_tElockDumper*, de Mr.Ocean, y *MKTVBDebugger* de Mr.Silver y Mr.Snow.[146]

5.6.3. Estudio Colectivo de Desprotecciones



El 25 de junio de 1998 nació un proyecto muy cercano a las ideas de WkT: el Estudio Colectivo de Desprotecciones (ECD), que puso en marcha en solitario **XixiaH**, después Mr.Brown: quería recopilar tutoriales y demás información sobre ingeniería inversa para ofrecerla al público.

> Inicié la página hacia 1998, con algunas explicaciones prácticas sobre cracking, pero sin los cracks propiamente dichos para evitar el cierre por parte de Geocities, donde la alojé**[147]**

Pronto se creó buena sintonía con WkT y ambos proyectos unieron fuerzas en enero de 1999**[148]**, con la implicación personal de Mr.WhiTe, quien seguirían encargándose del proyecto cuando Mr.Brown lo abandonó, un año después.

En la portada de la web de ECD + WKT, un curioso texto justificaba el crackear programas por la mala fe de los fabricantes de software, cuyas protecciones negaban a los usuarios el derecho a modificar lo que habían comprado:

> Este site nace con el objetivo de recopilar tutoriales en castellano sobre el noble arte del cracking, para de esta manera favorecer el aprendizaje de las técnicas de debugging, imprescindibles para defendernos de los bugs (mayormente intencionados, o sea protecciones) que los fabricantes de software introducen en sus programas, que no lo olvidemos, residen en nuestro disco duro, por lo cual deberíamos ser libres de poderlos modificar a nuestro antojo.**[149]**



Portada del sitio Estudio Colectivo de Desprotecciones en 1998, antes de unirse a WKT.

5.6.4. La rivalidad con TNT

Dentro de la escena hacker global, la del warez es de largo la que alberga más rivalidades, sea por ver quién es el grupo que saca más cracks o, en pleno siglo XXI, quién libera más películas. En esta carrera a nivel mundial, Whiskey kon Tekila llegó a estar entre los 20 mejores, explica Mr.Snow:

> Habia una gran competencia por sacar cracks como churros, se estaba en un ranking donde WKT llego a puntuar entre los 20 mejores del mundo. Pero no me preguntes en que se media esto, creo ke era la faceta mas "ilegal" del grupo y la que llevava black, él tenia relaciones con muchos grupos que nos daban Bouncers,ftps y demas.**[150]**

Había también pullas, a veces guerras, con algunos grupos en concreto. El enemigo número 1 de WkT era **TNT!Crack!Team**[151] que nació en 1999.



Lo más curioso de aquella guerra es que, según las versiones coincidentes de Mr.Jade[152] y Mr.Snow, los líderes de ambos grupos, Mr.WhiTe y **XasX**, se conocían en la vida real, siendo posiblemente amigos del mismo pueblo que competían desde sus grupos. La lucha fue feroz, como pudo comprobar Mr.Snow, que de TNT se pasó a WkT:



> Yo fui reclutado por TNT y su fundador XasX. Tras un tiempo en este grupo pude darme cuenta que habia gran pique con WKT hasta el punto que un dia WKT publico un CRACKME con el cual podias acceder al grupo si lo rompias, en este crackme salia una referencia del tipo "Si no puedes con él prueba en TNT" hahaha , eso sento mal por lo tanto me mandaron "Crackear" ese crackme. No recuerdo como paso exactamente pero xasx publico mi ensayo sobre ese crack y claro eso fastidio todo el trabajo de WKT ya que se exponia una completa solucion. Bueno como fuere no me gusto lo que hizo xasx y acabe entrando en WKT.**[153]**

5.6.5. El fin

2001 es la fecha oficial de la muerte de Whiskey kon Tekila. Parece ser que sorpresivamente no hubo peleas ni hechos traumáticos: simplemente, el grupo languideció. Como dice Mr.Snow, sus integrantes se hicieron mayores y ya está:

> Se fue dejando, yo personalmente en aquella epoca tendria entre 17 y 20 años vamos un crio y al igual que yo la mayoria, supongo que white no tendria el tiempo suficiente y lo iria dejando al igual que hicimos el resto. No existio conflictos ni nada por el estilo creo ke simplemente nos hicimos mayores o empecemos a salir de casa ;)**[154]**



Lo mismo afirma Mr.Jade:

> WKT murió desatendida, después de dos o tres intentos de revivir un monstruo que funcionaba por inercia, y sinceramente creo que lo mejor fué dejarlo morir poco a poco, sin traumas. Cada uno aprovechó el inpass para encontrar su sitio en otro lado y todos continuamos con nuestras cosas**[155]**

5.7. Los foros FxP

Junto al cracking, en los 90 avanzan también los métodos para distribuir los productos crackeados, primero juegos y programas, después música y películas. Nacen los foros FxP, cuyos miembros usan File eXchange Protocol (FxP) para almacenar y distribuir el warez. FxP es un método de transferencia de datos que utiliza el protocolo FTP (File Transfer Protocol**[156]**). Permite subir y bajar archivos de un servidor remoto a otro, sin pasar por la conexión del cliente**[157]**, consiguiendo una gran velocidad.

Estos servidores son usualmente servidores hackeados, de universidades o empresas que no saben que están siendo usados como repositorios de warez. Más adelante, con el intercambio de películas, se alquilarán los servidores de forma legal y se dotarán de potentes conexiones.**[158]**

Los foros de FxP son auténticos grupos organizados. Según la Wikipedia, "difieren del resto por el hecho de tener una membresía muy selectiva, permitir el acceso público por un tiempo limitado y cerrar hasta próximo aviso"**[159]**. En ellos, cada miembro tiene su función: los *escaneadores* rastrean Internet a la búsqueda de ordenadores vulnerables, con conexiones potentes a la red. Cuando encuentra uno, pasan la información a los *hackers*. Estos asaltan el ordenador y le instalan un servidor de FTP. Por último, los *fillers* (suministradores) introducen el warez en el servidor atacado, via FxP.

Lluís Ridao, antiguo miembro de un foro de FxP, explica el funcionamiento:

> Lo del FxP era un programa que te hacía un escaneo de IPs y, a través de los famosos "bugs" de Internet Information Server (IIS) de Microsoft, ejecutaba un exploit en cada uno de los IIS. A través de aquí, tenías que crear un FTP en otro puerto que no fuese el 21. Finalmente, se entregaba la IP del servidor asaltado a una persona que le metía todo tipo de programas y se hacían los intercambios mediante IRC o foros. Uno de aquellos grupos era http://pc-fxp.tripod.com/pc101.htm **[160]**

Ridao considera a estas comunidades antepasadas del P2P:**[161]**

> La gente entraba en un grupo de IRC o foro web y antes que nada tenías que darte a conocer con un nick, aportando alguna cosa. Tal como lo recuerdo, la persona estaba en varios grupos y se iban intercambiando la información de grupo a grupo, ya fuera una IP para añadir programas, que es lo que hacía yo, o gente que añadía las últimas novedades de programas,

MP3s… Puede decirse que sería una comunidad p2p pero ilegal.**[162]**

Estos foros, como muchos sitios de Internet dedicados a bajar y subir warez, la mayor parte de veces robado a la *Scene*, tenían lo que se llama “ratio de programa” que significa que, para bajar algo, había que subir otro archivo de similar valor.

6. Notas

1. ↑ Hacker. *Jargon File*
2. ↑ Ingeniería Social 1.0. LeStEr ThE TeAcHeR
3. ↑ Análisis de virus: anti-tel. Fernando Bonsembiante
4. ↑ Historia Oculta de Internet a través de sus personajes. *Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet. Andreu Veà Baró. Tesis Doctoral (12-09-02)*
5. ↑ Hackerz. Mercè Molist para el suplemento "Vang" de "La Vanguardia" (1997)
6. ↑ Hackerz. Mercè Molist para el suplemento "Vang" de "La Vanguardia" (1997)
7. ↑ EN LINEA CON... LeC. Hendrix. SET 18 (03-02-99)
8. ↑ Jfs en conversación privada
9. ↑ Hispahack, la película. *Mercè Molist para "Ciberpaís"*
10. ↑ Transcripción del comunicado del experto. Hispahack: tres "cerebros" desactivados. La Guardia Civil detiene a 3 presuntos "intrusos" informáticos españoles e imputa a otros 10. Mirta Drago. Diario del Navegante "El Mundo" (04-04-98)
11. ↑ Application:ICMPush.
12. ↑ LEGIONS OF THE UNDERGROUND RESPONDS. 2600 News (07-01-99)
13. ↑ Declaración conjunta de 2600, The Chaos Computer Club, THE CULT OF THE DEAD COW, !Hispahack, L0PHT Heavy Industries, PHRACK , PULHAS y T0XYN, *Mentes Inquietas* (07-01-99)
14. ↑ La resistencia se reúne en Berlín (29-12-98)
15. ↑ Un pirata desvía la página "web" de la Guardia Civil a otra homosexual. Mercè Molist. "El País" (01-12-98)
16. ↑ Valdivielso bromea sobre el ataque a su web. Pedro de Alzaga. Diario del Navegante. "El Mundo" (12-12-98)
17. ↑ Fallo en la web de la G. Civil. !H. *Mentes inquietas* (17-01-00)
18. ↑ Noticias. Segunda época (10-10-99)
19. ↑ Un hacker catalán gana el reto de 'PCWEEK'. Una-al-día, Hispasec (08/10/99)
20. ↑ Internet Zona Peligrosa. Miguel Ángel Nieto y Carlos Lapuente. Documentos TV. Televisión Española 2 (23-01-00)
21. ↑ Sin perdón. David de Ugarte. Bitácora de las Indias (01-08-03)
22. ↑ Manifiesto conjunto sobre la AIH, t0s (01-01-03)
23. ↑ Manifiesto conjunto sobre la AIH, Kernel PaniK
24. ↑ Hispahack se disuelve. Decowar (16-01-04)
25. ↑ _TaNiS_ en conversación privada
26. ↑ Vuelve Iberhack. Saqueadores Edición Técnica 11 (25-09-97)
27. ↑ Primer aniversario. El Nuevo Eljaker. Especial SET CON. SET (02/11/97)
28. ↑ CPNE RULEZ!. Web de la CPNE. Mirror en Internet Archive
29. ↑ Que es la CPNE (Compañia de Phreakers Nacional de España)??. Web oficial de CPNE (08-02-98)
30. ↑ Phreaking. Wikipedia
31. ↑ Phreaking. Patxi Astiz. S21sec labs (19-11-08)
32. ↑ PHUNTRICKS EN ESPAIN. El Jomles. SAB-MAG 0
33. ↑ Historia del phreaking en España. Phreaking. Wikipedia
34. ↑ - Que es un phreaker?. Web oficial de la CPNE (08-02-98)
35. ↑ ¿Que es un phreaking?
36. ↑ La CPNE. Web oficial de CPNE (08-02-98)
37. ↑ *"Underground.es, el underground español en Internet"*. Javier Pedreira "Wicho". **iWorld**, 7 (Julio/Agosto 1998)
38. ↑ Investigación y Desarrollo de la CPNE. Web oficial de CPNE (08-02-98)
39. ↑ El hacker, ¿experto o delincuente?
40. ↑ Warezzman, en conversación privada (19-01-12)

41. ↑ En línea con ArMaND VanHell. GreeN LegenD. SET 21 (08-11-99)
42. ↑ Historia del phreaking en España. Wikipedia
43. ↑ UMTS-TDD. Wikipedia
44. ↑ Llamadas con cargo a la Telefónica. Foro Hack Hispano
45. ↑ Chaping v2.0. TDD. Undercon 0x02 (1998)
46. ↑ CHAPING v. 2.5. Armand VanHell 08-02-99 (Version especial para RareGaZz). Raregazz 16
47. ↑ K.O. a los TM's. ISSUE 4 - Hark (06-03-98)
48. ↑ Anónimo (04-07-12)
49. ↑ PIC16F84A Data Sheet
50. ↑ Elmonta
51. ↑ Recorrido de una línea telefónica. TDD. Undercon 0x02 (1998)
52. ↑ "Descripción del recorrido que lleva a cabo la línea del teléfono". TDD. Internet Archive
53. ↑ [1]. Ripper. UNDERCON 0x02 (1998)
54. ↑ Que te puedes encontrar en un 900?. Hark. TDD. Undercon 0x04 (2000)
55. ↑ Seguridad Fisica en un TM. TDD. Undercon 0x08 (2004)
56. ↑ Aprende el funcionamiento de la Beige Box. La única que funciona hoy en día*. TDD*
57. ↑ Searched for http://www.webcrunchers.com/tdd/. Internet Archive Wayback Machine
58. ↑ En la cima de la Viruscene. Entrevista Mental Driller. Virus Attack (17-02-03)
59. ↑ Interview with Mr. Sandman. Bozo. VX Heavens.
60. ↑ Bernardo Quintero, en conversación privada (01-12-11)
61. ↑ Entrevista a Bernardo Quintero de Hispasec Sistemas. Un informático en el lado del mal (11-12-08)
62. ↑ Original de la entrevista a VirusBuster. Mercè Molist (24-07-02)
63. ↑ "No programamos por efectividad, programamos por originalidad". PC Actual (02-98)
64. ↑ 29A Issue #1
65. ↑ Interview with Mr. Sandman. Bozo. VX Heavens.
66. ↑ 40HEX. Textfiles
67. ↑ Los creadores de virus y la "Virus Scene". Javier Guerrero Díaz para PCManía (1997).
68. ↑ Los creadores de virus y la "Virus Scene". Javier Guerrero Díaz para PCManía (1997).
69. ↑ Mister Sandman. 29A Issue #1 (13-12-96)
70. ↑ Here we are :). 29A Issue # 1 (13-12-96)
71. ↑ Introduction. 29A Issue # 2 (13-02-98)
72. ↑ What is happening in IR/G?. Rajaat. 29A Issue # 2 (13-02-98)
73. ↑ Good bye!. Mister Sandman. 29A Issue # 3 (finales 1998)
74. ↑ Rajaats Resignation. 29A Issue # 3 (finales 1998)
75. ↑ Ithaqua. 29A Issue # 3 (finales 1998)
76. ↑ News. 29A Issue # 3 (finales 1998)
77. ↑ News. 29A Issue # 3 (finales 1998)
78. ↑ DDT: another group dies with its 1st issue. 29A Issue # 4 (03-00)
79. ↑ Membership. 29A Issue # 4 (03-00)
80. ↑ Words from Benny.29A Issue # 4 (03-00)
81. ↑ Words from the bee. 29A Issue # 4 (03-00)
82. ↑ Words from L.J.. 29A Issue # 4 (03-00)
83. ↑ Words from Prizzy. 29A Issue # 4 (03-00)
84. ↑ Win2000.Installer. 29A Issue # 4 (03-00)
85. ↑ '29A Issue # 5. (12-00)
86. ↑ Pirus. 29A Issue # 5 (12-00)
87. ↑ News. 29A Issue # 6 (03-02)
88. ↑ Membership. 29A Issue # 6 (03-02)
89. ↑ Introduction. 29A Issue # 6 (03-02)
90. ↑ Entrevista a VirusBuster. Mercè Molist (24-07-02) para Ciberpaís.
91. ↑ Situation in VX scene. 29A Issue # 6 (03-02)

92. ↑ The virmaking is dying. 29A Issue # 6 (03-02)
93. ↑ Last words from Benny. 29A Issue # 7 (02-04)
94. ↑ The Virus Underground. The New York Times (08-02-04)
95. ↑ Czech virus writer joins anti-virus firm. John Leyden. The Register (08-11-04)
96. ↑ He's got the virus-writing bug. Robert Lemos. CNET News (14-01-05)
97. ↑ SQL Slammer. Wikipedia
98. ↑ Benny. VirusInfo. Wikia
99. ↑ Police question man over Slammer worm. CNET News (01-12-04)
100. ↑ Mydoom. Wikipedia
101. ↑ News. 29A Issue # 7 (02-04)
102. ↑ News. 29A Issue # 7 (02-04)
103. ↑ News. 29A Issue # 7 (02-04)
104. ↑ Melissa. Wikipedia
105. ↑ Simon Vallor. Wikipedia
106. ↑ Gigabyte. VirusInfo. Wikia
107. ↑ Female virus-writer, Gigabyte, arrested in Belgium, Sophos comments. Press Release. Sophos (16-02-04)
108. ↑ VX Meeting Brno 2000. 29A Issue # 5
109. ↑ 29A Issue # 8 (01-01-05)
110. ↑ Trouble for 29A virus-writing gang as Russian member is sentenced, Sophos comments. Press release Sophos (18-11-04)
111. ↑ Old school VXers calling it quits. John Leyden. The Register (31-12-07)
112. ↑ 29A Web Oficial
113. ↑ 48bits interviews : Vallez/29A. Mario Ballano | 48bits (22-04-08)
114. ↑ 48bits interviews : Vallez/29A. Mario Ballano | 48bits (22-04-08)
115. ↑ Infamous malware group calls it quits. John Leyden. The Register (07-03-08)
116. ↑ Life in Saturn!. 29A Issue #1
117. ↑ Legal Stuff. 29A Issue #1
118. ↑ Policies and goals. 29A ezine
119. ↑ Claudio Hernández, en conversación privada
120. ↑ Claudio Hernández: "La gente ignora qué hay detrás de Internet". Mercè Molist (01-00)
121. ↑ Claudio Hernández, en conversación privada
122. ↑ Karpoff Spanish Tutor (30-06-02)
123. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002 (22-01-01)
124. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002. Parte Segunda (31-07-00)
125. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002 (02-10-00)
126. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002 (30-10-00)
127. ↑ Karpoff Spanish Tutor (02-04-02)
128. ↑ Cursos de Cracking Para Newbies. Ricardo Narvaja. Introducción Básica al Cracking. Manuales cracking de nuestra cosecha, para novatos. Karpoff Spanish Tutor 1999 - 2003
129. ↑ Registro de actualizaciones. Karpoff Spanish Tutor (23-09-01)
130. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002 (25-03-01)
131. ↑ FAQ sobre ingeniería inversa....1.0. Gerza (22-10-99)
132. ↑ Karpoff Spanish Tutor. Portada (12-01-03)
133. ↑ Registro de Actualizaciones de Karpoff Spanish Tutor 1999-2002. (11-10-00)
134. ↑ Karpoff y el cracking. Julio Verne. Arcón de la Historia. Joomla-GNU (31-12-09)
135. ↑ Comentarios para "Nostalgia (I)". X-Grimator. 48Bits (04-16-08)
136. ↑ 48bits interviews: MrJade/WKT! (07-13-08)
137. ↑ FAQ. *La página de Karpoff (22-10-99)*
138. ↑ Mr.Snow, en conversación privada
139. ↑ wkt-members. Whiskey Kon Tekila. Yahoo Groups
140. ↑ What happened with WKT?. RCE Forums (06-07-08)

141. ↑ Mensaje hoy inaccesible de Haplo en el antiguo foro de http://www.fwbz.net (02-09-05)
142. ↑ WKT Members (10-15-99)
143. ↑ [WKT!] Hall of Fame
144. ↑ FAQ Oficial de [WkT!]. Mr.WhiTe
145. ↑ FAQ Oficial de [WkT!]. Mr.WhiTe
146. ↑ Herramientas. La Página de Karpoff
147. ↑ Mr.Brown, en conversación privada
148. ↑ Unión con WKT. Novedades. Estudio Colectivo de Desprotecciones
149. ↑ Web de ECD tras la fusión con WKT, colección privada de Mr.Brown (09-01-99)
150. ↑ Mr.Snow, en conversación privada
151. ↑ TNT!CRACKERS REVERSE ENGINEERING AND SOFTWARE SECURITY GROUP (1999-2001)
152. ↑ 48bits interviews: MrJade/WKT!. 48Bits (07-13-08)
153. ↑ Mr.Snow, en conversación privada
154. ↑ Mr.Snow, en conversación privada
155. ↑ 48bits interviews: MrJade/WKT!. 48Bits (07-13-08)
156. ↑ File Transfer Protocol. Es.Wikipedia
157. ↑ File eXchange Protocol. Es.Wikipedia
158. ↑ Líneas dedicadas (T1, T2, T3). Kioskea.net
159. ↑ FXP board. En.Wikipedia
160. ↑ Lluís Ridao, en conversación privada
161. ↑ Peer-to-peer. Es.Wikipedia
162. ↑ Lluís Ridao, en conversación privada

7. Enlaces externos

REGLAS EN CANAL #HACK DE IRC ESPAÑOL. Privateer. Underhack.

7.1. !Hispahack

· Página web de !Hispahack
· Mirror de la web de !H
· Fermín J. Serna - Blog...
· Hacking contest spotlights many ways to attack Web sites, *CNN (03-11-99).*
· A practical vulnerabilty analysis (the PCWeek crack). Jfs. 1999.
· Hackeos Memorables: Jfs en el concurso de PcWeek. Security By Default (24/02/09)
· !Hispahack borrado de la Wikipedia. (06-08)
· «!H», no se sent, però si no hi és es troba a faltar.... Miquel Serrabassa. Entre silencis... (04-06-08)
· Hispahack se disuelve (10-02-04)

7.2.CPNE

· C.P.N.E.. Sitio oficial de la CPNE. Mirror en Internet Archive.
· CPNE - Diccionario de Términos. Gonchonet
· Hackers, los intrusos en la red. Laura Cortada. Revista Públic (06-00).
· Hackers, los intrusos en la red. Laura Cortada. Revista Públic (06-00). (mirror)
· CPNE detecta un fallo de seguridad en una web restringida en telefonica.es. LO + FUERTE, LO + ACTUAL, LO + CPNE. Sección hack de CPNE.
· Tarjetas de Timofónica. Portal Hacker.
· Manuales de Phreaking
· Métodos de hacking. Warezzman. SET 4 (02/11/96).
· Wardialing. Warezzman. SET CON Online (02/11/97).
· Códigos de barras. Warezzman. SET CON Online (02/11/97).
· MODO SECRETO DEL BEEPER COCACOLA By WaReZZMaN. CPNE (1997).
· Descripcion de las cajas de colores. Case Zer0. Iberhack.
· TRUCOS DE COMO LLAMAR GRATIS DESDE LAS CABINAS. CPNE
· DVB-Satellite Hacking for Dummies. Wzz. Undercon 2004.

7.2.1. Charlas de CPNE en la Undercon

· Codigos de Barras. Warezzman. Undercon 0x01 (1997)
· Stack Overflows. Dark Raver. Undercon 0x03 (1999)
· GSM Wardialing. Warezzman. Undercon 0x03 (1999)
· Hacking en entornos hostiles. Dark Raver. Undercon 0x05 (2001)
· Sistemas de comunicacion y navegacion aerea. Warezzman. Undercon 0x05 (2001)
· Barcoding. Warezzman.
· Reciclaje de Motorola. Warezzman. Undercon 0x06 (2002)
· Tecnicas de evasion para Netowork IDS. Dark Raver. Undercon 0x06 (2002)
· Heap overflows desmitificados. Dark Raver. Undercon 0x07 (2003)
· DirBiertete con DIRB - URL Bruteforcer. Dark Raver (The Old School). Undercon 0x08 (2004)
· DVB - Satellite Hacking. *Warezzman.* Undercon 0x08 (2004)

7.3. The Den of the Demons

· K.O. a los TM's. *TDD. HARK Issue 4 (06-03-98)*

7.4. 29A

· 29A Labs.
· Los creadores de virus y la “Virus Scene”. Javier Guerrero Díaz para PCManía (1997).
· 29A. VirusInfo. Wikia.
· 29A. Wikipedia.
· GriYo, un creador de virus. PC Actual (11-98).
· Charlando con GriYo. 7a69ezine (22-12-99).
· El retorno de Mister Sandman. PC Actual (03-00).
· Interview with Mr. Sandman. Bozo. VX Heavens.
· En la cima de la Viruscene. Entrevista Mental Driller. Virus Attack (17-02-03)
· Interview with The Mental Driller/29A by PetiK for PetiKVX Ezine #1.
· Entrevista a VirusBuster. Mercè Molist (24-07-02) para Ciberpaís.
· 48bits interviews : Vallez/29A. Mario Ballano. 48Bits. (04-22-08).
· Benny. VirusInfo. Wikia.
· Interview with Benny/29A. *-zine (Asterix) (12-99).
· Interview with Benny/29A by PetiK for PetiKVX Ezine #1.
· He’s got the virus-writing bug. Robert Lemos. CNet News (14-01-05).
· Interview with mandragore by PetiK for PetiKVX Ezine #2.
· Interview with Lord Julus by PetiK for PetiKVX Ezine #2.
· Lord Yup. VirusInfo. Wikia.
· Interview with Lord YuP. By PetiK for PetiKVX Ezine (28/05/02).
· En contacto con Wintermute. NetSearch. NetSearch Ezine #6 (02-07-01)
· The Virus Underground. Clive Thompson. The New York Times (08-02-04)
· Eugene Suchkov, 29A member, guilty of writing viruses. Sophos (18-11-04)
· Virus writers boast about Win 98 virus. CNN News (25-06-98).
· 29A dice adios…. Bernardo Quintero. Laboratorio Hispasec (29-02-08)
· 29A Labs has left the building. Pedro Bustamante. Panda Research Blog (27-02-08)
· Infamous malware group calls it quits. John Leyden. The Register (07-03-08).
· VXers Group 29A Calls it Quits. DarkNet (10-03-08).
· Encuentran al virus Cabir “in the wild” en los Estados Unidos. Guillem Alsina. DiarioRed (24-02-05)
· Cabir cell-phone virus was detected inside the US. Softpedia (22-02-05).
· Winux (Lindose). El primer virus para Windows y Linux. VSantivirus (29-03-01).
· Win32.Girigat. Giorgio Talvanti. Hispasec Sistemas.
· Introducción a la programación de virus bajo Win32. GriYo. VX Heavens.

7.5. La página de Karpoff

· Stomper
· Crack el Destripador
· Web de Ricardo Narvaja
· Lista de correo CracksLatinos

7.6. Whiskey kon Tekila

· Whiskey Kon Tekila -=The Original Spanish Reversers=-
· Estudio Colectivo de Desprotecciones
· COMO CRAKEAR POR ESTADO+PORCINO. Tripod.

8. Bibliografía

8.1. !Hispahack

· Fernández Palma, Rosa; Morales García, Oscar (2000), «El delito de daños informáticos y el caso Hispahack», en *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, ISSN 0211-2744, n.º 1, pp. 1522-1529.

· Ríos, Pepe (2000), *Primera sentencia por manipulación de datos en Internet: el caso Hispahack*, Iuris: Actualidad y práctica del derecho, ISSN 1137-2435, n.º 38, pp. 73-76

CAPÍTULO CUATRO

Information wants to be free

Information wants to be free

Cada generación de hackers dirá de los más jóvenes que han pervertido el arte del hacking, que no saben ni ponen atención, que son unos script-kiddies o unos vándalos hacktivistas. Y esto será así desde el principio, desde los viejos hackers de los 60, escandalizados ante la generación de los 90.

> Según Levy, las diferencias entre los viejos y los nuevos hackers son claras. El primer grupo se esforzaba por crear, el segundo se esfuerza por destruir y falsificar. El primer grupo amaba tener el control de sus ordenadores, pero el segundo ama el poder que le dan los ordenadores por encima de la gente. El primer grupo siempre buscaba cómo mejorar y simplificar; el segundo sólo explota y manipula. El primer grupo hizo lo que hizo porque había un sentido de verdad y belleza en sus actividades; el segundo grupo hackea por lucro y estatus. El primer grupo era comunal y muy unido, siempre compartiendo de forma abierta nuevos hacks y descubrimientos; el segundo es paranoide, aislado y secreto. Para Levy, los viejos hackers eran magos de la informática, pero los nuevos hackers son terroristas informáticos, siempre buscando nuevas formas de maldad o vandalismo electrónicos, sin pensar en las consecuencias.**[1]**

No le faltaba razón a Levy pero, más allá de la estética, las diferencias no eran tantas ni tan insalvables, como explicaba en un interesante texto el antropólogo Steve Mizrach:

> Los hackers de los 90 no son tan diferentes de los hackers de los 60, pues comparten los mismos impulsos libertarios, antiautoritarios y ansias de explorar; es sólo que los hackers de los 60 no entienden la situación en la que vivimos, probablemente porque se dedican a leer literatura hippie de los 60 y no ciencia ficción ciberpunk de los 90.**[2]**

Fuesen hippies o ciberpunks, hay un hilo invisible que une a los hackers de los 60 con la generación de los 90 y más allá, una vibración que les diferencia a todos del simple criminal: su ética. Se han escrito muchos documentos y libros sobre la ética hacker y aún hoy, en pleno siglo XXI, sigue vigente, siendo las más conocida la ética simplificada que, cual Moisés con sus mandamientos, Steven Levy mostró a la luz pública en 1984, en su libro Hackers, heroes of the computer revolution. Según Levy, estos son los puntos básicos del proceder, pensar, sentir... en definitiva, de la actitud del hacker:

> 1. El acceso a los ordenadores y a todo lo que te pueda enseñar alguna cosa sobre cómo funciona el mundo debe ser ilimitado y total. Da siempre prioridad al imperativo de poner las cosas en práctica.
>
> **2.** Toda la información debería ser libre.
>
> **3.** No creas a la autoridad. Promueve la descentralización.
>
> **4.** Los hackers deberían ser juzgados por su hacking, sin importar sus títulos, edad, raza o posición.
>
> **5.** Puedes crear arte y belleza con un ordenador.
>
> **6.** Los ordenadores pueden cambiar tu vida a mejor.**[3]**

De estos, el concepto más extendido, lema por sí solo de la cultura hacker, es: *Toda*

la información debería ser libre. En su nombre, la comunidad realizó un titánico esfuerzo de documentación, de forma gratuita, autoorganizada y alejada de cualquier canal oficial, para enseñar a los nuevos el camino del hacker, para mostrar la inseguridad de administraciones y empresas, para solucionar cualquier problema que pudiese surgir en aventuras tan impresionantes como el software libre y, ya en la era del puro hacktivismo de Wikileaks, para hacer pública información importante que los gobiernos han escondido.

Cabe aclarar que el imperativo de liberar la información nunca será un fuego a discreción y se aplicará con la precaución que demandaría Spiderman: Un gran poder conlleva una gran responsabilidad. Años después de la ética de Levy, desde Europa el Chaos Computer Club le pone coto: *La información privada debe seguir siendo privada, a no ser que tenga interés público*. Y es en este balance entre lo que puede liberarse y lo que no donde destaca el auténtico hacker, hijo de una comunidad que, a pesar de ostentar como meta la libertad de los datos, es también la que mejor sabe guardar un secreto, si la sagrada paranoia y el sentido común lo requieren.

El manejo de la información cubre pues diversos e intrincados niveles: la información que puede mostrarse totalmente al público, la que precisa ser liberada por etapas, o tamizada de forma que se escondan los datos privados de las víctimas (por ejemplo en robos de bases de datos). La información que se ofrece sólo en círculos privados, como puede ser una foro al que se entra por invitación o, más reducido, un grupo de amigos. Y la información que el hacker guarda sólo para sus ojos, que no explica ni a quien comparte el contacto más íntimo. Y es que por contar cosas a la novia ha caído más de uno, avisa ya en los 80 el estadounidense The Mentor, que Eljaker traduce:

> No comentes con nadie, a menos que sea de total confianza, tus hazañas. (Los más grandes hackers de la historia han sido cazados debido a las confesiones de sus novias)
>
> Cuando hables en bbs o por internet, procura ser lo más discreto posible. Todo lo que digas quedara almacenado.
>
> Se paranoico. Una da las características principales de los mejores hackers es la paranoia.
>
> No dejes ningún dato que pueda relacionarse contigo, en los ordenadores que hackers. Y si es posible, ni siquiera "firmes".**[4]**

Un aspecto muy debatido de la liberación de la información es el llamado *full disclosure*, que se refiere a si es pertinente avisar de fallos en sistemas sólo a sus dueños o hay que hacerlo extensivo a la sociedad. Y, en caso de ofrecerlo a un público amplio, si hay que esperar a que la empresa cierre el agujero antes de hablar. En 2002, este tema se debatía apasionadamente en la Noconname:

> La mayoría estuvo a favor de publicar los errores y concentró la discusión en la conveniencia de dar también el programa "exploit", que permite al administrador comprobar si tiene el fallo, pero también al intruso aprovecharlo. Uno de los asistentes afirmaba: "Yo y mis amigos no publicamos nuestros exploits, pero esto da un nivel superior para hacer daño, porque la gente no sabe que tiene el problema. Y, al final, como todos los secretos, acaba sabiéndolo

> medio planeta". La conclusión unánime era que "los exploits deben publicarse, pero no de forma irresponsable, no cuando hagan daño, dando tiempo a los fabricantes para reaccionar".**[5]**

Otro aspecto del *full disclosure* es el riesgo para el hacker que libera la información: más de una vez quien ha avisado a una empresa de agujeros en su red ha sido denunciado. Esto ha provocado que muchos opten por callar lo que descubren o, si lo creen necesario, utilicen canales que aseguren su anonimato. Problema parecido conlleva publicar según qué información en sitios web o foros públicos: en los años 90 era usual que los sitios web con "información hacker" mostrasen un descargo de responsabilidad parecido a este:

> Parte del material de esta seccion puede ser considerado moralmente reprobable e incluso ilegal en ciertos paises. Por ello los miembros de IBERHACK declinan toda resposabilidad del posible uso que se de a este material. La informacion contenida se facilita unicamente con fines educativos y/o cientificos. Presiona OK para continuar, o pulsa CANCEL para salir ahora.**[6]**

No menos importante, al otro lado del arcoíris, es la información que el hacker quiera dar de sí mismo, empezando por su rastro en las redes y ordenadores que asalte (algunos dejan una firma, Quickbasic dejaba incluso su teléfono, pero la mayoría borra sus huellas) y acabando por algo tan privado como son su nombre y su cara. Así como el hacker conoce y usa a la perfección las herramientas para divulgar la información, conoce y usa también como nadie las herramientas de privacidad, como el cifrado o los remailers anónimos, que esconden su identidad.

Después, en la práctica, la mayoría acabarán revelando su cara y nombre al grupo, incluso al público, pero unos pocos defienden con uñas y dientes su anonimato, cual lobos solitarios que necesitan la manada, sí, pero de lejos y sólo a través de la máscara, función que desempeña el *nick* o apodo, que a su vez puede esconder otro apodo, y otro, en un juego de espejos y muñecas rusas donde cambian los nombres pero siempre es la misma persona. O se usa un *nick* según se esté realizando una actividad u otra.

Mentes brillantes y frías las que pueden concebir y aguantar durante años este castillo de identidades en el aire, cuyo objetivo final no es más que obtener y divulgar la preciada información de forma segura para el hacker. Jugaron a esto la mayoría de veteranos que abrieron el paso a la tercera generación, algunos montando grupos cuyos integrantes jamás les conocieron en persona, como **Raretrip**, fundador de RareGaZz, un completo desconocido para quienes continuaron su obra:

> Raretrip me pasó todas las contraseñas para continuar con el trabajo de raregazz y desapareció del mapa.**[7]**

Algo parecido sucede con **eljaker**, fundador de SET, quien no se sabe nunca si se va o se queda, escondido tras múltiples apodos:

> **P -** Donde podemos encontrarte si queremos darte la paliza?

> **E -** En internet, aunque con muchos apodos, en el_duke@usa.net y en Murcia la mayor parte del año.
>
> Eljaker dura, y dura, y dura...**[8]**

Quien le hacía la entrevista, **Paseante**, brilló también por su anonimato paranoico, practicando el escapismo de su auténtica identidad con todo el “underground”, incluidos los componentes de la ezine que editaba, SET, quienes no conocían ningún dato que pudiese enlazar el apodo Paseante a una persona real.

Enfrascados en la replicación, traducción y producción de un montón de textos y ezines de aprendizaje de redes e informática, maestros de asignaturas que nunca se enseñaron en la universidad, guerreros de la luz que ofrecían a los novatos, convencidos de que la información debía circular por el mundo con la misma libertad con que circula por un ordenador... Sorprendía, tras tanta claridad, que muchos de sus textos**[9]** acabaran con una frase que se hizo mítica, sacada de una serie de televisión norteamericana: Tened cuidado ahí fuera, una advertencia que convertía de repente el blanco en oscuro, la luz en miedo y la libertad de la información en el toca de pies en el suelo.


En Portada

HACKERS

Especial sobre hackers de la revista “Jumping” en septiembre de 1997

En septiembre de 1997, la prestigiosa revista especializada en informática *Jumping* publicaba un reportaje sobre el fenómeno hacker, donde el periodista destacaba su interés por conseguir y compartir la información:

> Los hackers, cuya máxima pretensión (en su estado puro) es conseguir toda la información posible para divulgarla entre los demás usuarios (por lo menos en su reducido círculo de amigos). Hay que añadir que cuanto más grande sea el reto y más difícil sea conseguir esa información (independientemente del tipo o de la fuente) mayor será el aliciente para el

hacker.[10]

En este especial se reseñaban algunas de las primeras páginas que el “underground” tuvo en la web, como Underhack, Cyberhack, La Taberna de Van Hackez, Saqueadores Edición Técnica o The mafia magazine. Con mejor o peor calidad, con más o menos seriedad, estos sitios tenían en común el ser importantes nodos de difusión de información para la comunidad hacker, de dos formas:

Por un lado, los **generadores de información** en forma de traducciones y documentos aislados, que se replicaban primero de BBS en BBS y después de web en web. A mitad de los 90 ya son ezines, donde se recopilaban artículos generados por un grupo y sus simpatizantes.

Por otro lado, los **bibliotecarios de esta información**, que recopilaban documentos, programas y enlaces cual hormiguitas, los ordenaban y ofrecían en sus webs, faros de luz para el novato y el que no lo era tanto, bases de datos del conocimiento público de la comunidad hacker.

Las primeras webs hacker eran del segundo estilo, nodos que recopilaban y replicaban información, como hacían las BBS (de hecho, buena parte de su contenido procedía de las BBS). Iberhack fue uno de los primeros portales conocidos de información en castellano para hackers, en la web, creado en agosto de 1996. Ofrecía, como muchos que le seguirían, enlaces, documentos y algo de información propia, donde destaca el interesante texto Quien es quien en el mundo del hacking.

El creador de Iberhack fue **Warezzman/Hackman**, individuo polifacético donde los haya quien, casi al mismo tiempo, fundaba o co-fundaba la Compañía Nacional de Phreakers Españoles, la ezine Saqueadores Edición Técnica (SET) y el encuentro UnderCon.

En la sección de agradecimientos de Iberhack[11] vemos quiénes acompañaban a Warezzman en sus aventuras: **Eljaker**, co-fundador de SET; **Galahad**, del grupo Legión Oscura; **Fastdata**, que estará también en CPNE, y **Legion**, editor de Virtual Zone Magazine, la decada de las ezines hacker en castellano. Virtual Zone Magazine se hacía desde Granada. Nació en enero de 1996 y duró 5 números, hasta 2004. Versaba sobre temas de interés para programadores, como virus, demos, videojuegos...

1. Saqueadores Edición Técnica

SET ha sido la ezine más longeva de la escena hacker hispana, con 38 números. Algunos la han llamado la Phrack española. No en vano, pues llegó a tener gran influencia, no sólo la revista sino también las personas que congregó a su alrededor, siendo algunas artífices de buena parte de los proyectos de la escena hacker de los 90. Los artículos de la webzine de !Hispahack no tenían nada que envidiar a SET, pero fueron los segundos quienes triunfaron en el "underground" más castizo, de grupos, *cons* y noches en el IRC. Fue SET quien tuvo más "audiencia" y creó comunidad.

La ezine versaba sobre hacking, phreaking y temas relacionados. Nació con el nombre *Saqueadores* el 6 de octubre de 1996, en la *BBS Club* de Murcia. El primer número (en realidad los tres primeros números) sólo tenía un autor: **Eljaker**.





Hoy queda en pie su web oficial y un grupo de noticias en Usenet, abandonado: alt.ezines.set, que fue creado en diciembre de 1997.**[12]**

1.1. Cómo nació

Eljacker, **Warezzman** y **Dark Raver** crearon el grupo en agosto de 1996, en la BBS Club, según explicaría Eljacker:

> A finales del mes de agosto del a€o 1996 aparecio un extra€o mensaje en el area de hacking de BBS Club, tenia un logo formado por caracteres ascii y estaba realizado por alguien apodado Eljaker. Pretendia ser una especie de publicacion basada en temas del underground informatico.
>
> La historia comenzo unos meses antes, cuando un peque€o grupo de avezados informaticos habia elegido este area de mensajeria como lugar de reunion. El nivel era bastante bajo, pero ya empezaban a despuntar algunas habilidades destacables. El grupo estaba desorganizado y muchos de sus componentes preguntaban dudas que en ningun sitio encontraban respuesta.

> Por eso algunos de los mas veteranos en estos temas deciden fundar el grupo Saqueadores cuyo principal fin era distribuir entre los que deseaban aprender la informacion que pedian.
>
> Los tres miembros fundadores de este grupo fueron Warezzman, Dark Raver y como no, yo, Eljaker. Por aquel entonces eramos un grupillo de hackers novatos y con pocos conocimientos, pero con muchas ganas... y a la larga hemos demostrado que podiamos aprender muy rapido.
>
> Asi finalmente ademas de la activa conversacion en el area y el intercambio de informacion entre los componentes del grupo, se crean varias paginas webs y se decide sacar a la calle una publicacion.
>
> Los dos primeros numeros fueron una especie de ensayo, en teoria no tenian que haber salido de BBS Club, pero Warezzman decidio ponerlos en su pionera pagina del hacking hispano "Iberhack" y aqui empezo la carrera.**[13]**

Los primeros números, explica **alicuenca** en su *Historias de SET*, tenían un nivel muy bajo:

> De la mano de eljaker el primero numero solo trajo consigo un par de articulos escuetos que muchos no tardaron en denominar de infantiles.**[14]**

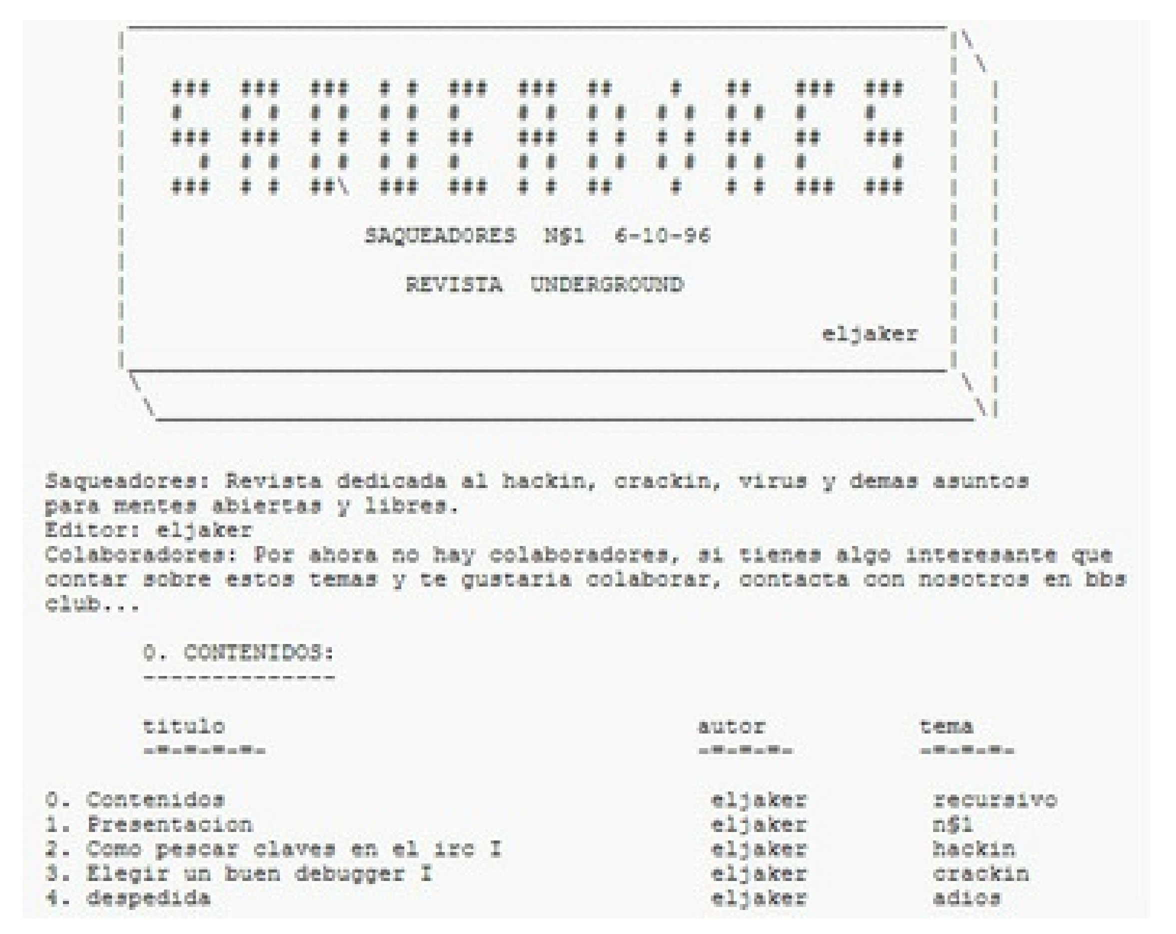
Es curioso que hubiese tan bajo nivel en esta y otras ezines aparecidas entonces, si tenemos en cuenta que la generación anterior había manejado conceptos e informaciones bastante más complejas. ¿Es que no hubo transmisión de información de una generación a otra?

No hay más que leer el Manual del novicio al hack/phreack que escribió Ender Wiggins en 1987, donde se explica por ejemplo cómo construir una blackbox. O las aventuras de LeStER y sus colegas de la *BBS God's House*, en los 80/90, usando alta ingeniería social (incluída exposición física) para conseguir teléfono gratis. O Glaucoma, descubriendo en 1989, mediante shoulder surfing, la contraseña de acceso a Iberpac... para darse cuenta del alto nivel al que llegó la segunda generación. Sorprende, 10 años después de tales hazañas, ver los primeros números de la que será revista bandera de la tercera generación, con artículos de primer curso de hacking, como robar contraseñas a los pobres usuarios del chat mediante burda ingeniería social.

Cabe recordar que, como explica eljacker, el bajo nivel en *Saqueadores* fue sólo en los dos primeros números, que no estaban pensados para hacerse públicos. A partir del tercero la cosa se pone muy interesante. Pero no es menos cierto que, observando la mayoría de ezines hechas por grupos españoles, salta la pregunta de qué pasó, por qué no se parte del nivel de Apòstols sino de nivel casi 0, por qué hay un abismo tan claro entre el hacking al que llegó la segunda generación y el punto del que partía la tercera. Hemos estado preguntando, pero no tenemos aún una respuesta que nos parezca cierta. La sospecha es que buena parte de la segunda generación *olvidó* educar a la tercera.

1.2. El primer número

Esta era la portada del primer número de Saqueadores:



```
SAQUEADORES  N$1  6-10-96

REVISTA  UNDERGROUND

eljaker

Saqueadores: Revista dedicada al hackin, crackin, virus y demas asuntos
para mentes abiertas y libres.
Editor: eljaker
Colaboradores: Por ahora no hay colaboradores, si tienes algo interesante que
contar sobre estos temas y te gustaria colaborar, contacta con nosotros en bbs
club...

        0. CONTENIDOS:
        --------------

        titulo                                  autor           tema
        -=-=-=-=-                               -=-=-=-         -=-=-=-

0. Contenidos                                   eljaker         recursivo
1. Presentacion                                 eljaker         n$1
2. Como pescar claves en el irc I               eljaker         hackin
3. Elegir un buen debugger I                    eljaker         crackin
4. despedida                                    eljaker         adios
```

Y estas eran las formas de contacto:

> BBS CLUB MURCIA 968-201819 y 968-201262
>
> y en internet en www.geocities.com/SiliconValley/park/7574/
>
> $$ Para contactar con nosotros, pasate por el area de hackin-crackin de
> bbs club o por el canal *#warezspain* (undernet) del irc, y pregunta por eljaker.[15]

1.3. La marcha de eljaker

A partir del cuarto número, en noviembre de 1996[16], eljaker dejó de publicar en solitario y aparecieron artículos de Warezzman, **El Duke de Sicilia**, **+Ochodedos**, **SLink**, **RoN**, **RedCool** y otros. La llegada de colaboradores coincidió con el cierre de BBS Club. Ahora la ezine se publicaría en diversas direcciones de Geocities, la web de Iberhack, Gorth BBS (Las Palmas de Gran Canaria) y DarkHate BBS (Girona).

Sorpresivamente, pocos meses después, en enero de 1997, Eljaker anuncia su retirada. La frase inicial del sexto número está escogida para ser su despedida:

> "There's no time for us,
> there's no place for us"
>
> Who want to live forever[17]

Según algunas fuentes, en realidad eljaker sólo cambia su nick a El Duke de Sicilia

[18] , práctica normal en el “underground” y que repetirá otras veces. Otros, en cambio, afirman que eran personas distintas.[19]

El fundador de SET escribe una carta de despedida donde explica que *Saqueadores* ha sido esencial para animar la escena hacker española:

> Cuando hace unos meses inicié la publicación, prácticamente en solitario y luego con un par de amigos, el hacking hispano estaba muerto. (...) Aunque había un par de grupillos mal organizados, no había casi documentos en nuestra lengua y (que yo sepa) no había ninguna publicación española. (...) Ahora, después de unos meses, parece que la semilla que plantamos empieza a crecer, ya hay varias publicaciones más, los canales del IRC sobre hacking en español están llenos, en las áreas de mensajería se empieza a hablar en serio, hay montones de páginas sobre hacking en español.[20]

Más adelante rectifica y aclara que sí existían otras publicaciones en castellano antes de SET, siendo la primera y más importante, argentina, Minotauro.

Coincide la marcha de eljaker con la publicación de nuevas normas en la revista: no tendrá fecha fija de aparición y quien escriba un artículo pasa a formar parte del grupo[21]. La sensación, pues, no es de disgregación de *Saqueadores* por huida del fundador sino todo lo contrario.

1.4. La redada de Isla Tortuga

En febrero de 1997, la ezine adopta el nombre de *Saqueadores Edición Técnica*. Aparecen de la nada los que serán sus nuevos pesos pesados: el **Profesor Falken** y **Paseante**. ¿Nuevas caras o sólo nuevos *nicks* de los fundadores?

El 27 de mayo de 1997 tiene lugar la redada contra Isla Tortuga, el más importante nodo de la comunidad hacker, pues allí residen buena parte de sus webs. El delito es presunta infracción de la propiedad intelectual por ofrecer warez en los sitios que aloja, concretamente *La página del jamón y el vino*. Algunos integrantes de Saqueadores están entre los detenidos y Paseante escribe el número de junio de SET en solitario:

> No obstante este brutal ataque contra quienes como nosotros difundimos información y no drogas ni armas ni pornografía infantil la revista NO VA a dejar de publicarse, este número es algo especial pues está hecho por una sola persona, Paseante, ya que los que no han sido detenidos están en estos momentos con las líneas de comunicación cortadas.[22]

Este importante episodio aparece también en las *Historias de SET*:

> Los dias mas oscuros de la zine pasaron por una redada de la G. Civil que acabo con la detencion de los miembros de Isla Tortuga ademas de los editores de la zine, incluyendo con ellos El Duke de Sicilia. Esta redada y las consiguientes detenciones supusieron la desaparicion de varias personas del ambiente Under y una temporada de paro para la comunidad entera.[23]

1.5. Época dorada

El hecho de mostrar que seguían vivos, en medio del tsunami que fue para la comunidad la redada de Isla Tortuga, afianzó al grupo dentro de la escena hacker.

Había empezado una nueva era, la época dorada, que se proyectaría al exterior en forma de nuevos miembros, la evolución del nombre de Saqueadores a SET y un cambio de diseño:

```
                 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                  Segunda Epoca - SET 12 - Noviembre 97
                 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA


                    Informacion libre para gente libre


              ///////////     ///////////    /////////////
              SSSSSSSSSS/     EEEEEEEEEE/    TTTTTTTTTTTT/
              SSSSSSSSSS/     EEEEEEEEEE/    TTTTTTTTTTTT/
              SSSS/           EEEE/              TTTT\
              SSSS///////     EEEE///////        TTTT\
              SSSSSSSSSS/     EEEEEEEEEE/        TTTT\
              SSSSSSSSSS/     EEEEEEEEEE/        TTTT\
                    SSSS/     EEEE/              TTTT\
              //////SSSS/     EEEE///////        TTTT\
              SSSSSSSSSS/     EEEEEEEEEE/        TTTT\
              SSSSSSSSSS/     EEEEEEEEEE/        TTTT\


                   Ezine del underground informatico


 ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
ÚÙÀ¿                                                                      ÚÙÀ¿
ÚÙÀ¿   Disponible en:   http://www.geocities.com/SiliconValley/8726      ÚÙÀ¿
ÚÙÀ¿                    http://vanhackez.islatortuga.com                 ÚÙÀ¿
ÚÙÀ¿                    http://www.thepentagon.com/paseante (puntero)    ÚÙÀ¿
ÚÙÀ¿                                                                      ÚÙÀ¿
ÚÙÀ¿ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -ÚÙÀ¿
ÚÙÀ¿                                                                      ÚÙÀ¿
ÚÙÀ¿   Editor:          Paseante <paseante@geocities.com>                ÚÙÀ¿
ÚÙÀ¿                                                                      ÚÙÀ¿
À»ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÀ»ÉÙ


 Recomendado: Editor de MS-DOS


AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
* ADVERTENCIA: La informacion contenida en este ezine no refleja la     *
* opinion de nadie y se facilita con caracter de mero entretenimiento,  *
* todos los datos aqui presentes pueden ser erroneos, malintencionados  *
* inexplicables o carentes de sentido.                                   *
* De aqui EN ADELANTE cualquier cosa que pase es responsabilidad        *
* vuestra. Protestas dirigirse a dev/echo o al tlf. 900-666-000         *
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

El Profesor Falken y Paseante lideran la revista, con artículos que harán historia, como una investigación de Paseante sobre vulnerabilidades en Infovía **[24]**

> Me gustaria que quedase claro que debido a la situacion espa€ola el control de Infovia posibilita el dominio cuasi-total del trafico Internet de nuestro pais, eso no es solo un atractivo innegable para un hacker sino tambien UNA RESPONSABILIDAD, no soy partidario de aquellos que en nombre de la “libertad” se dedican a desestabilizar sistemas ya que en definitiva nos acaba perjudicando por la perdida de servicios y la “leyenda negra” que se crea, ese es uno de los motivos por los que aqui damos pistas, indicios pero no todo masticado. El que quiera que se lo curre y por el camino confio que adquiera el sentido comun necesario para ser capaz de no hundir sistemas de los que dependen centenares de miles de personas.**[25]**

La excursión de Paseante por los servidores que forman Infovía tendrá gran repercusión, hasta el extremo que el artículo donde lo explica, en la *Saqueadores 11*, está actualmente desaparecido de la versión web oficial de la ezine (pero sigue vivo en el .zip original).

> El articulo sobre Infovia, la noticia ha volado fuera del mundo under (que fue el primero en enviar felicitaciones y palmaditas) y ha llegado a oidos de ISPs, Timofonica... Con mucha gente haciendo preguntas desagradables a la "Gran T" la compa€ia envio gente a la Undercon preguntando por los logs del Ascend (perdimos una ocasion de venderles una copia impresa) y las visitas a nuestras paginas de gente de Telefonica y el CERT demuestran que estamos en "el punto de mira".**[26]**

Aparecerán nuevos colaboradores: **+NetBuL**, **Garrulon**, **madfran**, **Green Legend**, **Rufus**, **Episiarca**. SET tiene cada vez más material y lectores. Es *La Ezine*.

1.6. UnderCon'97

Cuando la revista cumple un año, en octubre de 1997, lo celebran montando la Undercon, la primera convención del "underground" español, un encuentro público al que sólo se accede por invitación. Se celebra en Murcia el último fin de semana de octubre, dura tres días (24,25 y 26) y la organiza CPNE, cuyos líderes Warezzman y Dark Raver son cofundadores de SET. El coordinador es **Nexus_0** y el evento será una actividad paralela a la UNDERWEAR demo-party.**[27]**

SET sacó un número especial sobre la UnderCon**[28]** donde reaparecía momentáneamente Eljaker, firmando como **El Nuevo Eljaker**. La UnderCon'97 congregó a unas 60 personas de Murcia, Madrid, Alicante, Granada o León y grupos como La Vieja Guardia, CPNE, La Katedral e !Hispahack.

La UnderCon siguió celebrándose anualmente hasta el año 2004.

1.7. Hacking de altos vuelos

La mejor época de SET se alargará hasta aproximadamente el número 24, febrero de 2001. Es también la mejor época de la escena hacker española. Tres años de una orgía de buenos artículos, desde wardialing hasta paseos por redes militares, criptoanálisis, cracking Linux, intrusiones en redes IBM, Lotus, Iberpac, bancos, Cisco, inteligencia artificial, cursos, IRC War, IPv6, virus, PGP, GPS, phreak. El número 19**[29]**, en abril de 1999, llega a tener la friolera de 20 artículos. Se unen al proyecto colaboradores de gran calidad como **Hendrix** y **FCA00000**. Falken dimite como editor**[30]** y pasa el testigo a Green Legend, quien realizará esta función hasta 2002.

Una de las últimas acciones sonadas del grupo será el asalto al PacketShaper de Telefónica, un sistema que controla el tráfico de las redes de importantes empresas e instituciones españolas como Alcampo, Caja Madrid, "El País", "ABC", Instituto Cervantes, Telefónica, Banco Bilbao Vizcaya, Nestlé, Infonegocio, Agencia Estatal de Administración Tributaria, el Congreso de los Diputados, Iberia, Citroën y otros. Lo firma Paseante, cuyas hazañas lo han convertido en estrella indiscutible

de la revista.

> Que me pedia el cuerpo?.
>
> - Poner todo el trafico de Iberia a un _maximo_ de 1kb/s :
>   (...)
> - Crear una nueva clase de trafico en Correo_Telefonica para todos
>   los mensajes a Villalonga (tendra el correo ahi digo yo) y eliminarlos
>   sin avisar :-O
> - Vigilar todo el trafico que genera el servidor del Congreso a ver si
>   se esta haciendo buen uso de el
> - Guipar todas las sesiones Telnet y FTP (da mucho juego)
> - Numero 1: Aplicar un Redirect URL a la web de Telefonica.
>
> Que se esperaria de un 'piligroso delicuente hinfosmatico'?
>
> - Bloquear todo el trafico a El_Pais y el ABC
> - Resetear el PacketShaper, desconfigurarlo, cargar una nueva imagen delSistema Operativo troyanizada.
> - Dejar a todos los usuarios de Teleline sin servicio.
>
> (...)
> Podia haber hecho con el PS lo que quisiera, era completamente mio.**[31]**

1.8. La rivalidad con !Hispahack

Entre 2000 y 2001 empieza la decadencia de SET y un acontecimiento la marca claramente: su sitio web sufre diversos secuestros del dominio y un deface donde se demuestra que se han espiado las comunicaciones internas de algunos de sus miembros, que el atacante publica en el deface**[32]**. Aunque asegura que es miembro de SET, se pone en duda y las sospechas se dirigen a !Hispahack.

Es habitual en el "underground" que algunos grupos anden a la greña y SET no fue una excepción. En septiembre de 1998, alguien avisó a Geocities, donde se alojaba la web de la ezine, de que allí se mostraban contenidos de hacking, prohibidos por Geocities. Resultado: la web, en www.geocities.com/SiliconValley/8726, desapareció de la noche al día.

SET explicó posteriormente que la razón de este ataque fue un artículo publicado en la ezine #16, Real como la vida misma, donde se reproducían algunos logs de los canales #hack y #hacker que dejaban en evidencia a sus operadores.

> Nos acusaban de ser los responsables de unas detenciones producidas unos dias despues de publicar SET 16. Incluso nos denunciaron a Geocities... Lamentablemente para los que lo intentaron, ya estaba en marcha desde hacia tiempo el nuevo sitio.**[33]**

Aunque no se mencionaba abiertamente, quienes salían retratados en el artículo de la discordia eran un miembro y simpatizantes de !Hispahack y su grupo amigo, La Vieja Guardia, lo que convierte este episodio en una batalla más de la guerra entre los archienemigos SET e !Hispahack.

No está claro cuándo empieza esta rivalidad, pues en los inicios eran amigos.

Muestra de ello es que LeCréme, de !H, colaboró con Warezzman en la confección de las Páginas Grises y así se lo agradece el phreaker en el texto.

La cosa empezó a torcerse más o menos cuando SET inició el despegue. La primera referencia pública de *mal rollo* es el artículo humorístico *Visual Hacker 98*[34] que publica Paseante en noviembre de 1997 y molesta mucho a !H, como explicará LeCréme en una entrevista que publica SET en febrero de 1999. Según LeC, *Visual Hacker 98* es una parodia de la escena hacker que esconde en realidad una parodia de !H.

> Cualquiera que haya visitado Mentes Inquietas y sepa algo de !Hispahack vera que hay demasiadas coincidencias, muchas mas de las soportables para un texto como este, en relacion con !H. Referencias clarisimas a cosas que pueden leerse en la web, a actitudes que el presupone, o el color verde que aparece tantas veces...[35]

LeC también se queja públicamente de que en el artículo *Real como la vida misma* se haya reproducido un log en el IRC de un miembro de !H. Ahora SET no lo sabe, pero todo le será devuelto con creces en el futuro... Paseante responde a las acusaciones con un críptico texto que da a entender que algo pasó entre ambos grupos:

> Habria que remontarse al 97 y comenzar a recordar una relacion plagada de zancadillas, indirectas, pisotones y puñaladas traperas en la que, a menos que me haya perdido algun capitulo, NO empezamos nosotros.[36]

Sin piedad, Paseante escribirá otro texto sobre !H, entre la ironía y el reproche, cuando la Guardia Civil detiene a sus miembros en abril de 1998:

> Espero que salgan bien librados de todo esto, aunque no estaria de mas recordar a alguno de los "destacados" de !Hispahack ciertas actitudes y comentarios infantiles. (...) Comprendo que uno quiera ser el mejor y que ello lleve indefectiblemente a cualquier grupo español a 'medirse' con nosotros (que si nuestra web es mejor, que si yo hackeo mas que tu, que si nuestro ezine tiene mas colorinos...) pero aunque todos los grupos tengan el legitimo derecho de compararse con nosotros y autoproclamarse mejores (...) quiza, visto el resultado final, se podria haber optado por colaborar todos divulgar mas y mejor informacion y crear un autentico canal de comunicacion underground. La idea resumida seria: Menospreciar - y esforzarse +.[37]

Entre 2000 y 2001 la web de SET empieza a sufrir ataques que nadie firma, pero todos miran a !Hispahack. Hay diversos secuestros del dominio, que redirigen la web a otros sitios y, finalmente, un deface[38] donde se publican, oh sorpresa, *logs* de conversaciones públicas y también privadas en el IRC, donde Green Legend habla con diversas personas, amén de un listado de lo que se afirma es el disco duro de Green Legend, con mensajes de correo internos del grupo.

> En realidad el hackeo de la web fue un simple falseo (forge) de los cabezales del correo de la cuenta que aparecía en el whois del dominio en su momento. En el resto de ocasiones no fueron capaces de hacer más que intentos.[39]

A partir de aquí y al menos públicamente acabó la guerra entre SET y !H. En *Historias de SET* se da la versión del grupo:

> SET siempre tuvo y tendra enemigos, articulos, paginas y comentarios en contra de la zine los vereis siempre y si no daros un paseo por el tablon y vereis que Dios da manos a quien no las merece xd, pero uno de nuestros enemigos decidio llegar un poco mas alla y en el numero 26 madfran explico como uno de ellos logro hacer una buena escabechina con la web, decia ser un antiguo miembro... a mi tambien me parece que no.[40]

1.9. Decadencia

Después de Green Legend, los editores serán Madfran y Garrulo y los nuevos colaboradores, **blackngel**, **thenemi** y **elotro**. La revista tiene cada vez menos artículos y una periodicidad más irregular. Ya sólo se publican un par al año. SET empieza a escribir reportajes para la revista *@rroba* [41], por razones económicas:

> De alguna manera habia que financiar las actividades de SET y esta fue una de las menos malas.[42]

En el número 35[43], noviembre de 2008, se anuncia que hay un nuevo editor: Blackngel.

> Cuando todo parecia terminar, cuando en el horizonte no se veia mas que una linea indefinida e inalcanzable, cuando parecia que lentamente las fuerzas se agotaban y tan solo quedaba sentarse frente al monitor esperando que este se extinguiera por si solo, alguien ha pasado a nuestro lado y ha recogido el testigo[44]

En este número y los siguientes, firman artículos FCA00000, **Anay** y elotro, pero es blackngel quien escribe la mayoría. En octubre de 2009 es liberada la última SET, la 38[45], en la que sólo escribe blackngel.

A fecha de agosto de 2013, la web http://set-ezine.org sigue en pie.

2. RareGaZz

Junto a SET, destaca entre las ezines de hacking en castellano RareGaZz, creada en México y que siempre contó con hackers españoles entre sus editores y colaboradores. RareGaZz se ganó el respeto de la comunidad por la calidad de sus artículos, sobre todo a partir de que el alicantino **Guybrush** cogió el timón, a finales de 1997. La ezine aguantó 19 números, hasta 2002.

RareGaZz nació oficialmente en febrero de 1997, de la mano de **RareTrip**. Aglutinó a una amplia comunidad de hackers latinoamericanos y españoles, cuyos medios de comunicación eran la propia revista, la lista de correo RareDuDeZ, creada en 1996; el canal de chat #mano_izquierda en el IRC Hispano, y un sitio web que cambió diversas veces de alojamiento y del que se conservan unos pocos fragmentos en Internet Archive: http://raregazz.acapulco.uagro.mx/. En 2005, cuando la revista llevaba 3 años sin aparecer, se puso en marcha otra lista de correo, RareGaZz, que cesó su actividad en 2009.

En el primer número, Raretrip explicaba que su intención era liberar la información sobre hacking de los nichos elitistas[46]. Además y como característica diferenciadora, siempre hubo espacio para el hacktivismo en Raregazz, sobre todo en la primera época:

> Creiamos que encontrariamos dentro de esta zona llamada internet la utopia que Marx no pudo en la "realidad". Creimos eso y nos valio incluir textos sobre filosofia (...) y muchas otras materias que nada tenian que ver con la escena hacker excepto el tratar de crear conciencia usando como instrumento a la tecnologia. Funcionó[47]

Otro elemento único de la revista fue la mezcolanza de nacionalidades que participaron en ella, como explica uno de sus últimos editores, el peruano **ReYDeS**[48]:

> Empieza como un grupo mexicano y termina siendo un grupo Latinoamericano o Hispano, dado que teníamos miembros de México, Argentina, Bolivia, Uruguay, Perú, España y Chile. Eso sin contar la nacionalidad de nuestros colaboradores.
>
> El coordinar las reuniones via chat era un poco complicado algunas veces, dado que hablamos de gente en España y Latinoamérica. Había que encontrar horas que la gente estuviera lúcida y coordinar horarios praa reuniones de casi el 100% de integrantes algunas veces era imposible, así es que aprobábamos o coordinábamos las decisiones por mayoría simple algunas veces.[49]

2.1. Cómo empezó

La revista se gestó en 1994, en México, de la mano de RareTrip y sus amigos:

> La fecha exacta era esta: Carnaval 1994. (...) La conversacion? una discusion entre Pablo y yo sobre una revista que necesitaba ser creada. El tema? Hacking.
>
> En ese momento se decidio todo y se cometieron los primeros errores: RareGaZz seria un e-zine distribuido por correo electronico, jamas revelariamos nuestras identidades y nunca pero nunca cerrariamos la entrada a alguien.[50]

Esta era la portada del primer número[51]:

```
                    % % % % % % % % % % % %
                    %                     %
                    %      RareGaZz       %
                    %                     %
                    % % % % % % % % % % % %

                       *Introduccion*

Bienvenidos a la primera revista electronica  completamente  escrita en el
lenguaje de Cervantes dedicada a la comunidad Cibernetica del mundo entero
para dar a conocer lo relacionado a las computadoras, redes, programacion,
modos  de  vida, y  todo aquello  que se  relacione  con las computadoras.
En esta  edicion incluimos  dos buenisimos  articulos relacionados  con la
tecnologia Internet que te haran entender a profundidad como funcionan las
redes y la forma en que se comunican entre ellas.
En  las distintas secciones  de este MagaZine encontraras informacion util
tips  y sugerencias  para  mantener tu conocimiento sobre  computadoras al
maximo.
RareGaZz  es  una revista  publica  y  gratuita. Cualquier  persona  puede
colaborar para mejorar los bits que forman este E-Zine. La informacion que
aqui  encontraras te  servira  para hackerear distintos sistemas  y ademas
conoceras el ambiente de los Hackers Mexicanos y de todo el mundo.

                          NUMERO #1

       Temas incluidos:

       1.- Seguridad en su cuenta de Internet (RareTrip)
       2.- Trucos para mandar correo electronico (KillerBot)
       3.- Codigos para registrar programas Shareware (Dominio Publico)
       4.- Glosario de terminos usados en esta revista (raretrip)
       5.- Acerca de RareGaZz (raretrip)
       6.- L3t2 Hack! (raretrip)
       7.- Aplicaciones JavaScript para Home Pages (KillerBot)
       8.- Seccion de Software (raretrip)
       9.- La Guia completa para TCP/IP  1 de 2
      10.- La Conciencia de un Hacker por The Mentor -Traducido-
      11.- En el proximo numero...
```

2.2. La expansión

RareGaZz se distribuía a través de una lista de distribución de correo electrónico. Después se publicó también vía web, en una página de Geocities: www.geocities.com/Baja/4426.

> Se crearon los 2 primeros numeros y nos dimos a la tarea de crear listas de correo grandisimas usando algunos passwd's de universidades y de sitios como WhoWhere?. (…) Logramos como 100 peticiones del zine y despues se acabo. Frustracion total. (…) Me aferre mas a la idea y llego la solucion: Eureka! necesitabamos un webpage. Nacio la web page de RareGaZz en Geocities, vecindario Baja, numero 4426. Ahi aumento nuestra lista de personas que deseaban leer el zine y nuestro entusiasmo. Comenzamos a contactar gente, ellos a nosotros, mis compa~eros no lo creian. En Tijuana ya me conocian en las escuelas y sobre todo, mi rostro lo desconocian en todos lados.[52]

La revista se distribuía en media docena de sitios[53]. En cuanto a la web de Raregazz, cambió varias veces de sitio y dominio y estuvo, entre otros, en Isla Tortuga. Las dificultades por encontrar alojamiento se debían a que los contenidos de hacking estaban prohibidos en los servicios gratuitos.

Cuando RareTrip se fue del grupo, a principios de 1998, la lista de correo tenía unos 700 suscriptores[54] cuyas direcciones se perdieron y hubo que empezar de

cero. Esto no fue obstáculo para que en septiembre de 1998 hubiese en la lista RareDudeZz 500 suscriptores, lo que da una idea de su popularidad.[55]

2.3. Primera época

Firmaban textos en el primer número **RareTrip** y **KillerBot**. La mayoría era tutoriales muy básicos de hacking, ingeniería social o phreaking y artículos humorísticos y bizarros que corrían por los grupos de noticias. En las siguientes ediciones -hasta la 7- se les unen **Le Pompeltor** y **Mr. X** como "comandantes" y, como colaboradores, **Serverhacker**, **Raven Spirit**, **DuvaHazard**, **Dark Raver**, **Psycho Tranze**, **sir francis drake**, **Cracksmoker**, **Arkangel**, **Orion**, **Groovy**, **Carlos Truco**, **Yo**, **TucanX**, **NiK** y **RdK** (Red del Kaos).

```
El Grupo Revolucionarios del KaoS
            presenta

      \./\./ RAREGAZZ \./\./
```

Red del Kaos era un grupo autodenominado terrorista en el que estaba integrado RareGazz. Su líder, CrackSmoker, formó parte del "staff" de la ezine en los primeros números, hasta que desapareció:

> Somos un grupo de terroristas -si asi es- encargados de causar KaoS en los sistemas mexicanos reclamando democracia, libertad politica y sobre todo una mayor apertura a los grupos sociales como Rdk en los medios de comunicacion para transmitir nuestras ideas.[56]

En el número 7 aparece un nuevo colaborador, **Guybrush**, quien pronto estará en el "staff". Guybrush fue el primero miembro español de RareGaZz y abrió la revista a temáticas más técnicas, como puede comprobarse a partir del número 9[57] (finales de 1997), cuando RareGaZz empieza a parecer una ezine de hacking seria, con mejor edición, más artículos y, poco a poco, colaboraciones de grupos españoles: Underhack, JJF Hackers Team o más adelante TDD. En estos momentos, el "staff" oficial lo forman Arkangel, **Azumlord**, **Groovy**, Guybrush, KillerBot, Mr.X, **Orion**, RareTrip, ServerHacker y **VoV_77**.

2.4. Made in Spain

En febrero de 1998, Raregazz cumple un año y siguen llegando nuevos colaboradores, como **Yo_Soy** (quien más adelante se unirá a Raza Mexicana). El número 10 de la revista trae una explosión de artículos de temática violenta y antisistema, que aunque siempre han estado presentes, solían salir a uno por número. Ahora son diversos: *El foco bomba*, *Religión y otras cosas inservibles*, *La guía para joder cualquier automóvil* o un comunicado del Ejército Zapatista[58].

Es la traca final que antecede a la marcha por sorpresa de RareTrip y su equipo[59]. Guybrush será a partir de ahora el responsable:

> Raretrip me pasó todas las contraseñas para continuar con el trabajo de raregazz y desapareció del mapa ... tras su marcha hice reparto de funciones entre el resto .... web, lista de correo, ezine, etc ... continué con la misma política que se seguía al principio ... cada vez editaba uno el ezine.[60]

Los colaboradores de este número y los siguientes son casi todos nuevos y en su mayoría españoles, como **Nobody**, uno de los organizadores de la primera NoConName, en Mallorca. Guybrush hace notar el "desembarco" español en la Raregazz #16:

> Aclarar que RareGaZz tiene sus origenes en Mexico pero hoy en dia son todos en su mayoria espa€oles, aunque tambien contamos con miembros de otros paises como Mexico y Uruguay.**[61]**

La revista sigue subiendo el nivel técnico sin abandonar el espíritu didáctico que la caracteriza, pues buena parte de sus artículos son tutoriales, incluso empieza a incluir relatos sobre casos de hacking o cracking en directo, al estilo de SET. En septiembre de 1999 la periodicidad pasa a ser anual y se unen al "staff" **enan0** y **Aj0**.

Pero, en marzo de 2001, Guybrush explica en primicia a la revista NetSearch que abandona Raregazz, por problemas con el equipo:

> **<Guybrush>** ya no estoy en rare ... ni tampoco raretrip. raretrip volvio ... aparece en el ultimo ezine, pero ambos lo hemos dejado por ... diferencias con el resto.
>
> **<RaiSe>** pues es una pena.. y como es q estuvisteis tanto tiempo sin sacar rare17?.. y la perdida del dominio y eso?.. :?
>
> **<Guybrush>** el subdominio de acapulco lo perdimos porque parece que ese dominio ha desaparecido ... no se que rayos ha pasado y he perdido el contacto con los admins. Luego tardamos porque reuni un nuevo team y mientras nos organizabamos y la gente se decidia a colaborar ... paso algun tiempo. Resulta que la gente de ahora es demasiado cool y nada mas que quiere ser conocido y pertenecer a un grupo bueno pero nadie quiere trabajar ...
>
> **<RaiSe>** y tambien perdisteis la pagina web?.. lo digo pq estaba muy guapa.. mucha info y eso..
>
> **<Guybrush>** ahora hay una nueva web, pero supongo que raregazz ha muerto. nadie tiene ganas de trabajar, como te he dicho, tan solo quieren aparentar pero ninguno hace nada. Sin embargo, quieren tomar decisiones y mandar pero sin hacer nada a cambio ... despues de dar varios años a algo en lo que creia ... lo he tirado todo por la borda.
>
> **<RaiSe>** y el antiguo team?..
>
> **<Guybrush>** ni idea ... tan solo tengo relacion con raretrip.
>
> **<RaiSe>** entonces das una mala noticia.. ya es definitivo entonces?..
>
> **<Guybrush>** eso de mala notica es para algunos ... apuesto a que muchos se alegran. Si, es totalmente definitivo ... NUNCA volvere a formar parte de raregazz. De todas formas llevar un grupo es muy sacrificado ... la gente nada mas que sabe criticar..**[62]**

El último "staff" en el que aparece Guybrush lo forman él mismo, Raretrip, **Alt3kx_h3z**, enan0, **y0ni**, Yo_Soy, ReYDeS, **Ocsic**, Cytorax y **^Shadown^**.

2.5. This is the end

El 27 de marzo de 2002 aparece el último número de Raregazz, el 19[63][64], cuya editorial deja claro que es el final:

> La emision de una futura RareGaZz 20 resulta incierta de pronosticar. Pues como todos las personas 'normales'; los integrantes de RareGaZz, tenemos nuestras familias, estudios superiores, trabajos personales, etc. Y ello requiere mucho de nuestra dedicacion y tiempo.[65]

El último "staff" lo forman: Angel Protector, alt3kx_h3z, **Buanzo**, enan0, MagiCs, Ocsic, ReYDeS, ^Shadown^, **v1k1ng0** y Yo_Soy.

2.6. Hacktivismo

En su primera época, RareGaZz puede considerarse un primitivo grupo hackvitista, pues según cuenta RareTrip la razón de crear la revista es política: considera a Internet la *"utopía de Marx"* y a la revista un medio para *"crear conciencia"*[66]. La relación con Red del Kaos, autoproclamado grupo terrorista, lo radicaliza.

A mediados de 1997, en su número 4, Raregazz publica una convocatoria para atacar el Instituto Federal Electoral mexicano:

> CrackSmoker, lider temporal de RdK ha dado la orden a todos los miembros de RdK de intentar hackear el siguiente sistema: http://www.ife.org.mx para que el grupo gane popularidad y nos hagamos conocidos (mas) en toda la republica. (...) Que gane el mejor. RareTrip, KillerBot, Mr.X y LePompeltor trataran de no dejar abajo a los lectores de RareGaZz y haran todo lo posible para ser ellos los que entren y modifiquen ese sistema...imaginen nuestra grafica principal en ese sistema?[67]

Cuando la revista cumple un año, su lucha deja de parecer una broma de adolecentes para convertirse en algo serio: un acercamiento al Ejército Zapatista de Liberación Nacional y, más adelante, a los grupos que luchan por esta causa desde la tecnología. En el número 10 de Raregazz se publica el famoso *Comunicado del EZLN sobre la guerra en Chiapas México*[68] de diciembre de 1997.

El hacktivismo está naciendo en Latinoamérica de la mano del zapatismo. Los artistas Electronic Disturbance Theatre y el grupo mexicano X-Ploit organizan, entre 1998 y 2001, diversas netstrikes o manifestaciones virtuales en los sitios web de los gobiernos mexicano y estadounidense. RareGaZz no es ajeno a este bullir, incluso después de la marcha de RareTrip. En agosto de 1998, publica un texto que le ha mandado X-Ploit:

> Este es un comunicado de X-Ploit el cual fue enviado a -=RareGaZz=- y a otros medios de Comunicacion: We hacked with EZLN (MEX) on 4th february. (...) Durante un largo tiempo tuvimos un sniffer en la pagina del SENADO MEXICANO, esto es lo que obtuvimos, e-mails de los senadores.[69]

En el número 15 de la ezine, Guybrush entrevista a X-Ploit Team[70] que son los mexicanos LoTek, LeadRain y DES, cuyo principal objetivo hasta el momento ha sido asaltar sitios web del gobierno de México.

En este contexto, según Guybrush, la desaparición de Raretrip y su equipo a principios de 1998, justo cuando empieza la lucha hacktivista en su país, hace

pensar más en una nueva misión que en una retirada:

> En mi opinión, esta gente (los fundadores) estaban metidos en otros temas más turbios como puedes ver en los contenidos de los primeros artículos ... lo suyo creo yo que era más una lucha política y por esa época había otro grupo mexicano sin web pero bastante activo y conocido por atacar páginas del gobierno mexicano (X-ploit team) ... raro es que todos desaparecieran de golpe.[71]

2.7. Una detención

Hablando de ataques, un miembro del último equipo de Raregazz y de Raza Mexicana, alt3kx, fue detenido por la Agencia Federal de Investigación de México (AFI), en junio de 2003, acusado de haber atacado el sitio web de la presidencia de México. Según la acusación, alt3kx bombardeó el servidor con paquetes de datos de hasta 100 megabytes por segundo, que lo hicieron caer.[72]

Tanto RareGaZz como Raza-Mexicana[73] mostraron públicamente su rechazo a esta acción y a su autor.

3. 7a69ezine

Otra conocida ezine fue 7a69ezine, cuyo primer número aparecía el 9 de abril de 1999. Su fundador es **Ripe** y la revista nace llamándose **R|p3Hack**, pero a partir del cuarto número cambiará a 7A69. Durará 15 números, hasta 2003, y la portada del primero era esta:

```
R|p3HacK N$01
[ 09-4-99 ]
- GUIA PARA EL HACKER NOVATO -
Bajate cualquier numero de R|p3HACK en:                * By Ripe *
      < http://www.geocities.com/fashionavenue/Stage/1500 >
```

Ripe formaba parte del joven grupo The Net Team, cuyos integrantes eran, además de Ripe: **Tincho**, **Aule**, y **Cimos**. Este primer número contenía una presentación del grupo, un diccionario de palabras relacionadas con el mundo del hacking y un código ético copiado de la revista SET.

3.1. Cambio de nombre y consolidación

En el tercer número, 22 de mayo de 1999, llega el primer colaborador, **|CoDeX|**. En el siguiente, la revista cambia de nombre:

```
25-07-99
7A69
E-ZINE   (R|p3HACK n$4)       [By Ripe]
```

A partir de aquí 7A69 irá creciendo en calidad y cantidad de artículos. Entran más colaboradores: **IReick**, **Dan^^**, **AiNaKeR**, **Doing**, **Trycky**, **Relay**, **Tahum**, **Pollo1**. Se crea una lista de correo para avisar cuando aparece un nuevo número y se añaden más secciones, como la entrevista, que aunque será discontinua reunirá a interesantes personajes como GriYo**[74]**, del grupo 29A, JJF Hackers Team**[75]**; el Profesor Falken**[76]**, de SET, NecronoiD**[77]** y Cathack**[78]**.

> Bueno, como habeis ido notando el nivel de {7A69} ha subido progresivamente, de manera que cualquier persona puede adquirir ciertos conocimientos sobre hack y virii (y esperamos que en un futuro tambien algo de crack y phreak, todo se vera).**[79]**

Para celebrar su primer cumpleaños, la revista convoca un concurso de diseño de imágenes por ordenador**[80]**.

3.2. Canales de hack en el IRC de 1999

En el número 6 de 7A69 aparece un artículo que hemos creído interesante reproducir, sobre las tribus de la escena hacker que se movían por el IRC-Hispano a finales de 1999:

> **#hacker_novatos:** Debido al nombre (NOVATOS), muchos pueden pensar que en este canal solo se reune la "gerna" de hacking, pero he de decir que no es asi, el nivel en #hacker_novatos es igual (o incluso mejor :P) que el del resto de los canales, es decir, no demasiado alto :(
>
> **#hacker:** Tras unas epocas de crispacion y "mal rollo" entre algunos de los asistentes habituales a este canal (entre los cuales, por desgracia me incluyo yo), parece que las cosas han ido mejorando, y el ambiente que se vive en #hacker es medianamente bueno, aun que es demasido habitual ver siempre a los mismos.... y away (los hay que tienen tarifa plana, y se dedican a sobrecargar los servidores de IRC quedandose conectados las 24h).
>
> **#hack:** Aqui se reune la supuesta 31337 del hack español, si bien es cierto que puedes encontrar gente de autentico nivel, es un canal en el que es muy dificil integrarte.
>
> **#hack_novatos:** Algunas personas se empeñan en decir que los canales #hack_novatos y #hacker_novatos son "rivales". No se de donde habran sacado esa chorrada. Yo no entro en este canal, sin embargo lo he echo alguna vez, y he de decir que el grupo es algo mas reducido que el de #hacker_novatos (no quiero decir que sea peor).
>
> **#hacking:** Otro de los canales a los que no entro. Segun tengo entendido en este canal el nivel es mas o menos alto, sin embargo el grupo es bastante reducido.
>
> **#seguridad_inform tica:** (Con acento en la "a") Este canal esta mas bien dirido a gente que se defiende de los hackers, pero... šQue mejor que ser un hacker para defenderte de ellos? Por lo que aqui tambien encontraras algun que otro hacker de "nivel".
>
> (...)
> Ademas de canales dedicados al hack podemos encontar otros canales dedicados al mundo del undergr0und, entre ellos #virus (normalmente no muy poblado, tendras suerte si ves a mas de dos dentro), #phreak (no se habla demasiado), #crack (normalmente no se encuentra a nadie)...**[81]**

3.3. Segunda época

Cuando la revista está a punto de cumplir su segundo aniversario, adquiere un dominio propio: 7a69ezine.org. Hay cambios en el diseño y una mínima organización interna: Ripe y Trycky son los editores y el "staff", Tahum, Doing e IReick. En cuanto a los colaboradores, seguirán llegando y de calidad: **OverDrive** (Net Phreak Team), **PAC_MAC**, **[SnAkE]**, **Ja|0**, **tuxisuau**, **Jet-Li**, **Jafar**, **Anarion**, **Lykeios**, **Marconi**, **mnm**, **xuzato**, **Bruj0**, **Fkt**, **IaM** (The Old School), **bzero**, **N4XoR**, **ZiSXko**, **Memonix**, **ProdiX**, **QuasaR** (Undersec), **Viesllo**, **Acero**, **IcArO**, **tomac**, **pancake** (CatHack!), **Lindir**, **Pluf**, **esn-min**, **AbeToRiuS**, **Runlevel**.

Pero aunque no baja su calidad, la ezine tiene cada vez más problemas para salir. El número 15 es liberado el 23 de noviembre de 2003: ha tardado más de un año.

> Ha sido muy duro… Durisimo… Ha costado un monton… Nos ha costado MAS DE UN AÑO, pero seguimos aqui dando guerra y esperamos durar mas. **[82]**

A pesar de los buenos deseos, el 15 será el último.

4. La Taberna de Van Hackez

Al lado de los creadores de artículos y ezines están los recolectores y distribuidores de esta información, cuyas webs suelen tener más visitas que el sitio original. La presentación usual de estas bibliotecas es el directorio de enlaces, al estilo de los que triunfaban en aquel momento, como Yahoo! o Altavista. Los enlaces se ordenaban por temáticas y los visitantes podían votar las páginas según su calidad, votaciones que se reflejaban en más o menos estrellas para el sitio.

Los directorios de enlaces especializados en el mundo hacker ofrecían enlaces, textos, herramientas y los más grandes tenían zonas de comunicación para sus usuarios. Eran pequeñas BBS trasladadas a Internet que funcionaban como puertas de entrada, sitios de iniciación donde era posible encontrar rápidamente nodos y caminos a los que, de otra forma, habría sido difícil llegar.



índice de recursos de La Taberna de Van Hackez en 1999

Las primeras webs de este estilo fueron Iberhack en 1996; Underhack, desde al menos 1997, cuyo "staff" lo formaban **Privateer**, **AciDmaN**, **Crimson Tide**, **IPghost**, **Napalm**, **Schoddy Guy** y **Superbomb**; o Darkside, con un estilo diferente porque no ofrecía los datos ordenados en directorios sino empaquetados en el *DarKSIdE Hacking Pack*.

```
*******************************************************************************
\\//\\//\\//\\//\\//\\//\\DarKSIdE Hacking Pack v.1\\//\\//\\//\\//\\//\\//\\
***********************************D.H.P.**************************************
Madrid, 25 de Diciembre 1996
```

Pero será La Taberna de Vanhackez, del valenciano **El Replicante**, quien conseguirá más audiencia, tanto por su diseño como por el volumen de información que ofrece, además de foros y chats. Otros directorios que vendrán después, como Prehackers en 1998 y Elhacker.net en el 2000, seguirán su concepto.

La Taberna de Van Hackez nace, como mínimo, en 1997, ya que se cita el sitio en un artículo de la revista *Saqueadores*, publicado el 25 de septiembre de 1997:

http:// vanhackez.islatortuga.com - La Cueva de Van Hackez - Van Hackez viene con ganas y su pagina es completa donde las haya, una cosa que esta muy bien es que la mayoria de programas, revistas, textos estan directamente en su Web y no dependen de links que normalmente (Murphy rules) no funcionan. Como buena pagina esta siempre en construccion.**[83]**



Este fue el último logo de la Taberna, en uso entre 2002 y 2005

La Taberna estuvo un tiempo en Isla Tortuga: http://vanhackez.islatortuga.com y, a mediados de 1998, cuando la Isla desapareció a consecuencia de la denuncia de la Business Software Alliance, *El Replicante* compró un dominio propio: http://www.vanhackez.com.

4.1. Qué había en la taberna

Aunque fue ampliando secciones, la zona de H/P/C/W/V de La Taberna de Van Hackez no cambió mucho en los 7-8 años que estuvo funcionando. Ofrecía enlaces a crackeadores de contraseñas, anonimizadores, mailbombers, escaneadores de puertos, exploits, troyanos, emuladores de tarjetas telefónicas, generadores de tonos para “boxes”, generadores de números de serie para crackear programas, generadores de números de tarjetas de crédito, sitios donde tener correo o páginas web gratis, emuladores de juegos, scripts de IRC y otras herramientas de interés para cualquier hacker.

De especial interés histórico era la sección de textos**[84]**, donde había interesante documentación técnica en castellano, como el famoso Manual del Novicio al Hacking, del apóstol Ender Wiggins.

Entre las traducciones al castellano destacaban IP-Spoofing desmitificado, de IPgh0st, de Underhack, fechada en 1997, traducción de un artículo de Phrack. O La superguía del hacker, traducida por Nobody el 13 de enero de 1998. También Hackers: Rebeldes con causa y Guía del hacking (mayormente) inofensivo parte 1 y parte 2, traducciones del grupo B.B.K..

Había también textos jocosos, obligatorios en cualquier web de hackers que se preciase, como A VÉ ¿QUÉ COÑO’SUN HACKER?, firmado por **The Buscon of Astalavista**, o COMO SER UN “JAKER” EN 10 MINUTOS O EN 10 LECCIONES BREVES.

La mayoría de estos textos ya estaban en las BBS y los primeros directorios en la web, como Iberhack. Los sitios de este estilo solían copiarse los unos a los otros, pues el objetivo era tener cuanta más información mejor.

4.2. Copias de copias

Había muchas páginas personales que hacían lo mismo: copiar de los grandes directorios. Hasta aquí se toleraba, pues ellos mismos se copiaban también. Pero si

además ponían publicidad eran denigrados por la comunidad, que les echaba en cara ganar dinero con el trabajo de otros. La Taberna de Van Hackez se había quejado más de una vez de esos copiones y volvió a hacerlo cuando remodeló la web, en el año 2000:

> A esos sitios que se montan la web con los archivos de la taberna, se les acabó parcialmente el chollo, al menos de momento. A ver lo que tardan en volver a las andadas. Gran parte de los archivos de la antigua web ya no funcionan desde allí. Respecto a estos ruínes buitres de la praaderar nada que decir. Es fácil crear una web con gigas de archivos haciendo cut&paste ¿Verdad? El caso de Hackers Dark City Mexico es lo más patético que puede encontrarse en la red. Cientos o miles de enlaces buitreados de otras webs, como de la Taberna, de Canal Paranoia, de Hackers.com, de Tlsecurity, etc. Incluso el colmo del buitreo al enlazar con los archivos de Hack Hispano, que a su vez enlaza a los archivos de La Taberna. Impresionante ;). Y el caso es que tiene más visitas que todos los sitios que buitrea, claro, reúne todos los archivos de otras webs en la suya sin dar un palo al agua… Es para pensar si nos merece la pena mantener los archivos, pagar servidores, etc..**[85]**

Cabe decir que El Replicante tampoco era un santo: La Taberna había sido precoz en el uso de publicidad pornográfica para financiarse, la única que funcionaba entonces en Internet. La web tenía dos zonas claramente delimitadas: la de hacking y *La casa de madama Flop*, con pornografía**[86]**.

4.3. Los infames TVHCDs

Completaba el negocio la venta de CDS recopilatorios de herramientas y textos de hacking, los llamados TVHCD (Taberna de Van Hackez CD). En noviembre de 1999 se puso a la venta el primero, con 650 MB de datos, por 1.500 pesetas más gastos de envío**[87]**. Al año siguiente apareció una segunda versión, que costaba 2.000 pesetas**[88]**.

La comercialización de estos CDs levantó ampollas en la comunidad hacker, como podía leerse en es.comp.hackers, bajo el título *Vanhackez, pirata entre los piratas*:

> Este tipo se dedica a vender unos cds por 2000 ptas. (¿los hará con gasolina, y por eso son tan caros?) con supuesto 'contenido propio', que en realidad son textos y tutoriales que han sido hechos de forma desinteresada, y puestos a disposición de todos los internautas de forma gratuita. Entre ellos, se encuentran varios textos salidos de las entrañas de estos grupos (es.comp.hackers y es.comp.cracks). Por supuesto, para incluir estos textos en su cd no ha pedido permiso a ninguno de sus autores (doy constancia de ello). **Seldon**.

Por lo que parece, El Replicante hizo oídos sordos a las críticas y siguió vendiendo los TVH CDs**[89]**



La Taberna vivió una radical remodelación en el 2000 y cambió de logo

En 2004-2005 el canario **LeChuck** compró la web y la siguió actualizando durante un tiempo hasta que, a finales de 2005, la Taberna desapareció. Por aquellas fechas, el foro tenía alrededor de 2.700 miembros[90].

En los últimos meses de su existencia sólo se podía acceder a la portada, donde había el siguiente texto:

> "Lo que no me mata, me hace más fuerte". Friedrich Nietzsche.
>
> Volveremos…[91]

5. Notas

1. ↑ Old Hackers, New Hackers: What's the Difference?. Steve Mizrach
2. ↑ Old Hackers, New Hackers: What's the Difference?. Steve Mizrach
3. ↑ Hackers, heroes of the computer revolution. Steven Levy.
4. ↑ Curso de hacking empezando desde cero I. Eljaker. Saqueadores 5 (20/12/96)(*Nota: Eljaker no lo especifica pero muy posiblemente es una traducción de* A Novice's Guide to Hacking- 1989 edition*, de The Mentor*)
5. ↑ Un centenar de expertos en seguridad se reúnen en Mallorca. Mercè Molist para "Ciberpaís" (29-07-02)
6. ↑ Web de Iberhack
7. ↑ Guybrush, en conversación privada
8. ↑ En línea con eljaker. Paseante. SET 16 (16-09-98)
9. ↑ Manual del Hacker , para newbies,cybernovatos y para internautas que no saben de que va esto. pRoYeKto nAkArkO 1997-2002
10. ↑ Jumping. Especial HACKERS. Rafa Daroca (09-97)
11. ↑ Informacion sobre esta pagina: Colaboraciones, sugerencias, e informacion. Iberhack
12. ↑ Proposal of alt.ezines.set. Miguel Angel Tellez. 06/11/97
13. ↑ Primer aniversario. El Nuevo Eljaker. SET Especial Undercon (02/11/97)
14. ↑ Historias de SET (bazar), alicuenca. Saqueadores Edición Técnica, 31 (06-05)
15. ↑ Despedida. Saqueadores 1 (06-10-96)
16. ↑ Saqueadores 4. 02/11/96
17. ↑ SAQUEADORES N.6 (10-01-97)
18. ↑ En línea con eljaker. Paseante. SET 16 (16-09-98)
19. ↑ Ha nacido HackStory.net
20. ↑ Mensaje de Eljaker. Saqueadores Edición Técnica 6 (10-01-97)
21. ↑ Renovación del grupo y de la revista. SET Staff. SET N.6 (10-1-97)
22. ↑ -importante-. Saqueadores Edición Técnica, 9 (15-06-97)
23. ↑ Historias de SET (bazar), alicuenca. Saqueadores Edición Técnica, 31 (06-05)
24. ↑ Infovia?. Oui c'est moi. Saqueadores Edición Técnica, 11 (25-09-97)
25. ↑ Infovia?. Oui c'est moi. Saqueadores Edición Técnica, 11 (25-09-97)
26. ↑ Editorial. SET 12 (08-12-97)
27. ↑ UNDER CON '97 Primer Congreso Underground. Panorama del hack hispano. SET 11 (25-09-97)
28. ↑ Especial Undercon. SET (02-11-97)
29. ↑ SET 19 (29-04-99)
30. ↑ Editorial. SET 20 (18-08-99)
31. ↑ El último paquete. Paseante. SET 21 (08-11-99)
32. ↑ SET hacked. Historias oscuras de SET, recopiladas por terceros (no demasiado imparcial)
33. ↑ Real como la vida misma. SET Staff. SET 17 (19-11-98)
34. ↑ Visual Hacker 98. Paseante. SET 12 (08/12/97)
35. ↑ EN LINEA CON... LeC. Hendrix. SET 18 (03-02-99)
36. ↑ EN LINEA CON... LeC. Hendrix. SET 18 (03-02-99)
37. ↑ La importancia de llamarse hacker. Paseante. SET 14 (16-04-98)
38. ↑ SET hacked. Historias oscuras de SET, recopiladas por terceros (no demasiado imparcial)
39. ↑ Elmonta
40. ↑ Historias de SET (bazar), alicuenca. Saqueadores Edición Técnica, 31 (06-05)
41. ↑ Articulo publicado por SET en @RROBA. SET 27 (01-04-03)
42. ↑ Historias de SET (bazar), alicuenca. Saqueadores Edición Técnica, 31 (06-05)
43. ↑ SET 35 (01/11/08)
44. ↑ Editorial. SET Staff. SET-35 (01/11/08)
45. ↑ SET 38. (10-09)
46. ↑ Que es RareGaZz?. Raregazz 01

47. ↑ RareGaZz 17. Requiem por RareGaZz. Raretrip (12-00)
48. ↑ Proyectos. Alonso Eduardo Caballero Quezada aka ReYDeS
49. ↑ ReYDeS, en conversación privada
50. ↑ RareGaZz 17. Requiem por RareGaZz. Raretrip (12-00)
51. ↑ RareGaZz 01
52. ↑ RareGaZz 17. Requiem por RareGaZz. Raretrip (12-00)
53. ↑ Magazine. Fragmento de la web de RareGaZz conservado por Internet Archive Wayback Machine (12-10-99)
54. ↑ RareGaZz a finales del año 1997. Raregazz 09
55. ↑ La RareDudeZz esta cerca de los 500 usuarios. Raregazz 14 (09-98)
56. ↑ CTRL + ALT +DEL. Raregazz 03
57. ↑ Raregazz 09
58. ↑ Raregazz 10
59. ↑ Introducción. Raregazz 12 (1998)
60. ↑ Guybrush, en conversación privada
61. ↑ Editorial. Raregazz 16 (09-99)
62. ↑ En contacto con Guybrush. RaiSe. NetSearch Ezine #5 (02-03-01)
63. ↑ Raregazz 19. (27-03-02)
64. ↑ Lanzamiento RareGaZz 19
65. ↑ Editorial. Raregazz 19 (27-03-02)
66. ↑ RareGaZz 17. Requiem por RareGaZz. Raretrip (12-00)
67. ↑ CTRL + ALT + DEL. Raregazz 4
68. ↑ Comunicado del EZLN sobre la guerra en Chiapas México. Raregazz 10
69. ↑ Comunicado de X-Ploit. Raregazz 13 (08-98)
70. ↑ Entrevista a X-Ploit Team. Guybrush. Raregazz 15 (11-98)
71. ↑ Guybrush, en conversación privada
72. ↑ Cae pirata que atacó web de la presidencia de México. VSantivirus (28/11/2003)
73. ↑ Arresta PGR a alt3kx. Staff Raza-Mexicana
74. ↑ 7a69 07
75. ↑ 7a69 08
76. ↑ 7a69 10
77. ↑ 7a69 13
78. ↑ 7a69 14
79. ↑ 7a79 07 (22-12-99)
80. ↑ 7a69 08 (12-03-00)
81. ↑ 7a69 06 (24-10-99)
82. ↑ 7a69 15 (23/11/03)
83. ↑ Panorama del hack español. Saqueadores 11 (25-09-97)
84. ↑ Textos Hacking. La Taberna de Van Hackez (09-10-99)
85. ↑ ¡Al Rico Chorizo Oiga!. *Roko. La Taberna de Van Hackez (16-10-00)*
86. ↑ La casa de madama Flop. La Taberna de Van Hackez. Web Archive (01-12-98)
87. ↑ TVH CD-1. La Taberna de Van Hackez
88. ↑ TVH CD-2. La Taberna de Van Hackez
89. ↑ La tienda de Van Hackez
90. ↑ TVH Foro. La Taberna de Van Hackez (20-03-05)
91. ↑ La Taberna de Van Hackez. 19/02/05. Web Archive

6. Enlaces externos

· Microsoft quiere limitar la divulgación de fallos informáticos. Mercè Molist para “Ciberpaís” (14-11-01).

6.1. SET

· Página web de SET
· Historias de SET. Saqueadores Edición Técnica, 31 (01-07-05).
· El underground español en Internet. iWorld, 7 (07-01-1998).
· La web de Falken. Internet Archive.
· Paseante: “Lo hago porque puedo”. Mercè Molist para “Ciberpaís” (05-07-01).

6.2. RareGaZz

· En línea con: GuyBrush. Saqueadores Edición Técnica, 15 (20-06-1998)
· Recopilación de todas las ezines de RareGaZz. ReYDeS.
· Recopilación de todas las ediciones de RareGaZz. Govannom, Seguridad Sistemas Informáticos.
· Hackers y algo más. Hacking. Raregazz.
· Bugs. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· IRC. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· Magazine. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· Hacking. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· AIX. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· Disclaimer. Fragmento de la web de RareGaZz. Internet Archive Wayback Machine.
· Lista de correo RareDuDeZ
· Lista de correo RareGaZz

6.3. La Taberna de Van Hackez

· Referencia a Van Hackez. Entrevista El-Brujo de Elhacker.net.
·

CAPÍTULO CINCO

La comunidad

La comunidad

“Que es mi ordenata mi tesoro
que todo el mundo ha de temer.
Mi ley, el ratón y el módem.
Mi única patria, la red”

Canción del Pirata. *Adaptación anónima del poema homónimo de Espronceda*

El Jargon File es un glosario en inglés sobre la jerga hacker. Lo inició un estudiante de matemáticas de la universidad de Stanford, Raphael Finkel, en 1975, como recopilación de términos usados por diversas comunidades técnicas: ARPANET, los laboratorios de Inteligencia Artificial de Stanford y el MIT y otras universidades norteamericanas.

El *Jargon File* era y es un archivo online[1] y tan vivo como la revolución a la que pertenecía, abierto a nuevas incorporaciones de palabras a medida que estas se afianzaban en las diversas comunidades que estaban creando Internet. Uno de sus colaboradores más fieles fue el creador del software libre, Richard Stallman. Desde 1990, el conocido programador Eric Steven Raymond (ESR) administra esta joya de la comunidad hacker.

Según el *Jargon File*, la definición de ética hacker es como sigue:

> Creencia en que compartir información es un bien poderoso y positivo. Hay un deber ético entre los hackers de compartir su experiencia, escribiendo código abierto y facilitando el acceso a la información y los recursos computacionales, siempre que sea posible. Grandes redes como la misma Internet pueden funcionar sin control central por este trato, en el que todos confían y que se refuerza con un sentido de comunidad, que podría ser su recurso intangible más valioso.[2]

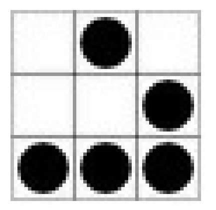
Efectivamente, la Comunidad de los hackers es su activo más valioso pues, a pesar de lo que digan las películas, el hacker no es un enfermo asocial, al contrario, necesita relacionarse, pero con gente como él. Muchas historias reales de hackers recuerdan al patito feo del que todos se ríen hasta que, viendo a unos cisnes, descubre que también lo es. Para muchos hackers las redes han sido los cielos donde han descubierto a sus hermanos, denostados en el Mundo Real como gafotas, empollones, niños hiperactivos, retraídos y etc.

La ética hacker es la sangre que corre por las venas de esta comunidad. A efectos prácticos, en los foros coge el nombre de Netiqueta, unas pocas normas de comportamiento[3] que aseguran la buena salud de la interacción, la sagrada interacción entre personas que es la base de la red. Sin policía, sin gobiernos e, idealmente, sin nadie que modere, sólo con unas pocas normas consensuadas de forma horizontal, anónima y global.

Algunos viejos hackers han tratado de explicar con palabras qué y cómo es esta su

comunidad, tan intangible como potente. No es fácil pues hablamos de un grupo de alcance mundial que ha podido cohesionarse a pesar de las diferencias de cultura o idioma. Eric S. Raymond lo hizo bastante bien en su libro La catedral y el bazar, donde se centra en la comunidad del software libre pero cuyas palabras puedes extrapolarse a toda la comunidad hacker:

> Aunque la programación sea una actividad solitaria, los auténticos logros surgen de la puesta en común de la atención y la capacidad intelectual de comunidades enteras. Aquel que dependa tan sólo de su cerebro al desarrollar un sistema va a estar siempre en desventaja frente al que sepa cómo crear un ambiente abierto y en evolución en el cual la búsqueda de errores y las mejoras se confíen a cientos de personas.**[4]**



Emblema hacker

Un ejemplo de cómo funciona esta comunidad sería la instauración del emblema hacker: Raymond escribió una propuesta a la comunidad, que mandó a algunos foros, cuyos contertulios lo mandaron a otros, hasta que llegó prácticamente a todos los que estaban en aquel momento a la escucha. Ningún comité jerárquico lo aprobó: simplemente, el hecho de que la comunidad empezase a usarlo lo convirtió en emblema oficial.

Otro ejemplo sería el modo de funcionar de una de las instituciones más viejas de la red, la Internet Engineering Task Force, creada en 1986. La IETF es un grupo autoorganizado y planetario de personas que trabajan de forma voluntaria en la creación de nuevas tecnologías para Internet, que en la mayoría de ocasiones acaban siendo estándares técnicos. No tiene una junta directiva, ni miembros, ni cuotas. Su funcionamiento se basa en reuniones, a las que puede asistir y opinar cualquiera.

> Muchas veces, la IETF sigue las ideas de sus miembros. Una de las "ideas fundacionales" está plasmada en una vieja cita de David Clark sobre la IETF: "No queremos reyes, presidentes o votaciones. Creemos en el rudo consenso y el código corriendo".**[5]**

La comunidad hacker no está localizada en un sitio concreto sino en muchos, dentro y fuera de Internet, recordando a las Zonas Autónomas Temporales que glosó el escritor anarquista Hakim Bey, en 1991**[6]**.Programas diseñados por los propios hackers crean estos territorios libres, sitios online donde nacen, viven y mueren las comunidades que forman la comunidad.

La materia prima de esta cuerpo hecho de muchas células es la conversación. Hay cientos, miles, decenas de miles de comunidades de gente intercambiando información, organizadas según la temática de lo que se discute en ellas. Eso fueron los foros de las BBS, los grupos de noticias, y siguen siendo las listas de correo, los canales de chat, los foros en la web, los grupos de Facebook, Twitter... La comunidad no existe, no es nada sin las conversaciones, la comunidad muere si enmudecen los

foros.

Esta vida online se traslada muchas veces al Mundo Real, para salir un poco, verse, respirar, reír juntos o hacer el amor. Desde el principio de los tiempos las redes han propiciado citas físicas entre quienes trabajan -o viven- en ellas. Son lo que el chat bautizó como *kedadas*, reuniones en las que participan quienes frecuentan la misma pequeña comunidad online. También existen las convenciones o *cons*, un legado del mundo científico y universitario que inventó la red. Suelen ser anuales y agrupan a mayor número de personas, integrantes de las diferentes comunidades que comparten un mismo tema de interés, por ejemplo los expertos en seguridad informática o los webmasters, dentro de la Comunidad.

1. Undercon

La UnderCon es el primer encuentro más o menos público de hackers españoles de diferentes grupos. Se celebró anualmente en Murcia desde 1997 hasta 2004. Nació como fiesta del primer cumpleaños de la revista SET pero, visto el éxito, se le dio continuidad.



La UnderCon se celebraba en octubre, aprovechando el Puente del Pilar, y la organizaban la CPNE -Warezzman, Dark Raver, Fatuo...- y su grupo adyacente La Katedral. Se accedía por estricta invitación y era preciso tener un alto nivel técnico para ser invitado.

> Este requisito no pretende convertir el evento en una reunion “elite” sino que su objetivo es garantizar un nivel basico de concienciacion y de implicacion en la escena underground. (...)
>
> Si alguien quiere pertenecer a un grupo / comunidad / escena como minimo debe preocuparse de formarse, estudiar, aprender y comprender, la base tecnica y la jerga del underground. El hacking / under no es solo una estetica es una forma de pensar y de ser...**[7]**

El hecho de haber sido invitado un año renovaba automáticamente la invitación al siguiente y daba también autoridad para invitar a nuevas personas.

> Podeis invitar a todas aquellas personas de vuestra confianza, interesadas en estos temas y con conocimientos suficientes para aportar algo. Pero es muy recomendable que actueis con discrecion, no queremos publicidad en ezines, publicaciones o informativos de cualquier tipo.**[8]**

Se recomendaba discreción también sobre la localización de la reunión. No era algo gratuito, pues entre los temas de las charlas los había claramente delictivos o muy delicados: cómo contratar fraudulentamente líneas 905 y 906, como conectarse gratis a Internet, como enviar SMS gratis por móvil, cómo programar virus, intercambio de tarjetas de crédito robadas...

A partir de mayo de 2003 el congreso tuvo dominio propio: www.undercon.org. Actualmente esta dirección alberga contenidos no relacionados con el mismo. Es posible acceder a los textos antiguos en Internet Archive: http://web.archive.org/web/*/http://www.undercon.org

1.1. La primera UnderCon

Empezó llamándose SETCon y se realizó en octubre de 1997, como fiesta del primer aniversario de la ezine, que sacó un número especial sobre el evento[9]. Congregó a unas 60 personas de Murcia, Madrid, Alicante, Granada o León, de grupos como La Vieja Guardia, CPNE, La Katedral, Raregazz e !Hispahack. Las personas que no habían podido asistir, como algunos de Cyberhack, conectaron vía teléfono o IRC.

> Se hablo mucho de los 900 con acceso a internet de IBM, de Samsung e incluso de los de Telefonica y Microfost... Tambien se hablo de las tarjetas chip (smartcards). Se hablo de hacking, como no. El articulo de los ascend de paseante fue la estrella. Tambien se hablo bastante de linux, para que os hagais una idea el 90% de los asistentes eran usuarios de linux, un buen sintoma...
>
> Por supuesto no faltaron las criticas a Microsoft y a Telefonica. La dudosa seguridad de los NTs y del protocolo NetBios fueron base para muchos chistes. (...) Los objetivos del evento se cumplieron, se establecio un contacto entre los componentes de la escena hack/phreak y se sentaron las bases para futuras convenciones.[10]

Según la crónica de SET, esta fue la lista parcial de asistentes: Dark Raver (Saqueadores / CPNE), Entropia, Warezzman (Saqueadores / CPNE), Darkcode (Vieja Guardia), Necronoid (Vieja Guardia / Hispahack), FastData (CPNE), Flecha, Dairo Bel (Vieja Guardia), Fuego Fatuo, Fit0 (Vieja Guardia / Hispahack), Overdrive (Net Phreak team), Shou, Sauron, Mainboard, Gotcha, Fateros, Ufo, Pipo, Netdancer, Jcl, Pleyade, Pesca, Senpai, GuyBrush (Raregazz), Cain Garcia, Ric3, Kloniko, Kemo, Lord_lt, Axel, D_hunter, Bishop, CaseZer0, Eljaker (Saqueadores).

1.2. ¡Qué viene la policía!

La segunda edición de la UnderCon[11], en 1998, congregó a más grupos[12], como los respetados creadores de virus 29A, los expertos en phreaking de cabinas telefónicas The Den of the Demons (TDD) y **Com30**, quienes se harían famosos dos años después porque su detención propició la Operación Millenium, la mayor redada por phreaking en España.

Así como en la primera edición, en esta también se habló[13] mayoritariamente de phreaking (escuchar conversaciones ajenas en Motorola, interceptar mensajes de *beepers*, pinchado de cabinas, uso ilegal de números 900 de empresas para acceder gratuitamente a Internet, como usar gratuitamente el teléfono desde la caja de pares de un edificio). Los teléfonos móviles, por aquel entonces ladrillos con antena, fueron los absolutos protagonistas, explicó Ripper de TDD, en su crónica:

> A cada momento libre que habia se empezaba a hablar sobre moviles, estrella invitada a esta UnderCon '98 :), ya que la densidad de movil por metro cuadrado fue brutal, para que os lo imagineis el 95% de la gente que fue alli llevaba movil.[14]

Hubo también espacio para la seguridad en comunicaciones inalámbricas, virus, redes X.25 o un taller para interceptar las frecuencias de radio de la policía, en el que los asistentes se llevaron un gran susto:

> Entraron corriendo The3rdMan y Legend al local diciendo que todos fuera, metieron el grupo electrogeno en el local, y todos salimos rapidamente pero de forma ordenada, cosa que me dejo muy sorprendido y eso me demuestra que tenemos bastante sangre fria, ya ke lo

normal hubiera sido una estampida general :), pero al salir no vimos a la policia, a los 3 o 4 min los vimos aparecer, entonces nos preguntabamos que como sabian que venian para el local, y entonces fue Warezzman quien nos hizo una clase practica del uso del scanner.

Habia estado escuchando la banda de la policia local y oyo como enviaban un coche patrulla al local, pero cuando llegaron fue demasiado tarde y habiamos desaparecido todos :)**[15]**

1.3. UnderCon III: La definitiva

Fue en la tercera edición[16], en 1999, cuando la cosa empezó a ir en serio: ¡Por fin había sillas!, ¡y mesas!, ¡y electricidad!:

Las mesas se llenaron rapidamente de todo tipo de ingenios electrónicos.[17]

Dark Raver llamó a esta UnderCon *"la definitiva"***[18]**. Asistieron unas 60 personas, entre ellas nombres propios de la escena hacker hispana que acababan de llegar o repetían, como **Demons Paradise**, Guybrush, Senpai, **+NetBul**, **Hendrix**, **Shooting** (el abogado Carlos Sánchez Almeida), **Joy**, **Sage**, el grupo TDD, **Binaria**, **Mortiis**, **GriYo**, **Zhodiac**, **Net_Savage**, Overdrive, **Crono**. Incluso, como contó GreeN LegenD **[19]**, hubo alguna empresa que fue a buscar talentos.

En cuanto a las charlas, esta vez el phreaking no fue el rey. Se habló también de hacking, carding, electrónica, radioafición, lockpicking, ingeniería social, programación, UNIX, wardialing, routers, virus, certificados digitales, seguridad en redes inalámbricas, pinchar líneas GSM...

1.4. Clase magistral



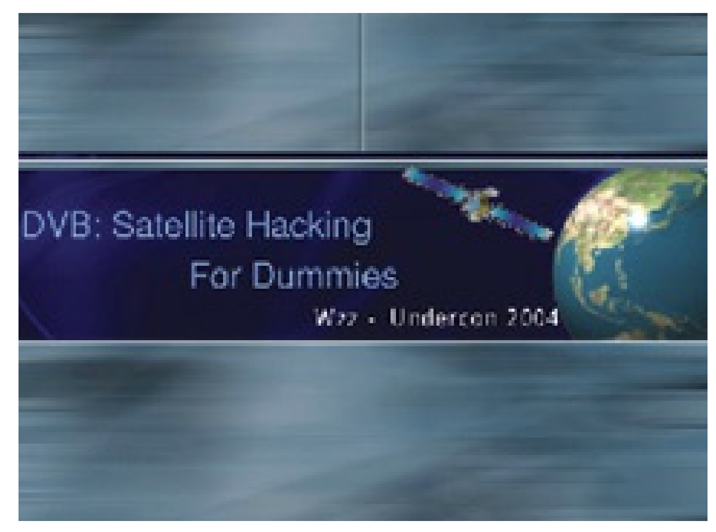
Charla de Warezzman en la Undercon 0x05 (2001)

Hay poca información pública sobre el resto de ediciones de la UnderCon. Gracias a una crónica de Kriptópolis tenemos noticias de la cuarta**[20]**, en el año 2000:

Altísimo nivel en phreaking y networking, con una clase magistral a cargo de Homs: se sale de su ponencia destripando routers. Los magnates del pago por visión hubiesen pagado por escuchar cómo se monta -y desmonta- una red de cable: decodificar la señal de parabólica es demasiado fácil.

La mayoría de las conferencias fueron puro código. Con todo, la nueva legislación de

protección de datos tuvo su hueco. No es de extrañar, considerando que estaban allí reunidas las empresas y grupos de hackers que realmente cuentan en el mercado.**[21]**



Charla de Warezzman en la última Undercon

A partir de la quinta edición, en 2001, el evento fue decayendo igual como decaía todo el “underground”, pasando de ser una *con* a una reunión de 20 amigos. Junto a los habituales -Fuego Fatuo, Dark Raver, Warezzman, Griyo de 29A y el grupo TDD-, impartieron sus conocimientos en esta última época Zhodiac, **Sp4rk**, **MaDj0kEr**, **Slayer**, DarkCode, **Kekabron**, **Pope**, **Zert**, **Pof**, **Lorenzo Hernandez**, **IaM**, **Pluf** y **Pancake**.

La octava UnderCon**[22]**, en 2004, fue la última. Su página web, que estuvo en pie hasta 2012, exhibió durante años un mensaje donde “amenazaban” con volver: Seguimos Vivos.

1.5. Fotos

Las fotos oficiales de la UnderCon tenían la originalidad de mostrar no las caras sino los teléfonos móviles de los asistentes. Son un buen recuerdo no sólo de la *con* sino también de la evolución que vivieron estos aparatos en pocos años:



Foto oficial de la UnderCon 2 (1998)



Foto oficial de la UnderCon 5 (2001)



Foto oficial de la UnderCon 8 (2004)

2. Isla Tortuga

Isla Tortuga nació en 1996 como un portal que ofrecía espacio web gratuito para los cada vez más grupos hacker hispanos. Muchos habían visto como Geocities y otros servicios de alojamiento gratuito eliminaban sus páginas por *contenido ilegal* y no dudaron en apuntarse a la comunidad de la isla. Durante sus dos años de existencia fue el mayor navío de la flota pirata hispana, llegando a alojar a 68 grupos, entre ellos !Hispahack, La Vieja Guardia, RareGaZz, VanHackez, Underhack, Iberhack, Ciberhack, CPNE o 29A.



Portada de Isla Tortuga en enero de 1998

El servidor donde residía Isla Tortuga, sito en Estados Unidos, pertenecía a la empresa de Barcelona Vesa Tecnologías, propiedad de Angeloso, un viejo conocido de la comunidad warez, y Maki, actuando como comercial y técnico respectivamente. Una de las líneas de negocio de Vesatec era crear páginas en Internet que tuviesen mucho tráfico, cara a ponerles publicidad pornográfica y lucrarse con la misma.

La primera página que alojó Isla Tortuga, *Viva el jamón y el vino*, era su joya de la corona, con 2.800 visitas diarias en febrero de 1998, según el folleto que Vesatec mostraba a sus clientes:

> La pagina más famosa de España en cuestion de visitas. Incluye fotos Erotico-pornográficas del sexo femenino y gran cantidad de programas desprotectores. Todos los servicios que se ofrecen en ella son totalmente gratuitos. **[23]**

El *Jamón* eran fotos pornográficas, el *Vino* eran aplicaciones para desproteger programas y había una tercera sección, los “Likores”, con programas para romper contraseñas. **Fer13** administraba la página.

2.1. El Caso Vesatec



Maki. Esta es su única foto pública disponible en Internet

El 27 de mayo de 1997, la Unidad de Droga y Crimen Organizados de la Policía Nacional detuvo en Barcelona a Angeloso, de 30 años, y Maki, de 29. Se les acusaba de *"delito continuado contra la propiedad intelectual por facilitar gratuitamente herramientas para acceder a programas de ordenador y generar números falsos de tarjetas Visa y American Express"*.



Angeloso, en 2007

Más tarde, el 2 de julio de 1997, la policía detuvo en Madrid a Fer13, quien se declaró responsable de la página del *Vino*, objeto de la denuncia. Pero los denunciantes, las empresas Autodesk, Lotus, Adobe, Novell y Microsoft, tras la fachada de la Business Software Alliance, mantuvieron sus acusaciones contra Angeloso y Maki, por alojar la página. Otras personas no implicadas directamente pero vinculadas al "underground" fueron también detenidas.

El juez obligó a cerrar el servidor donde se alojaba Isla Tortuga, que estuvo fuera de servicio una semana. La policía incautó 7 ordenadores, 2 portátiles (Intel DX4

100Mhz), 4 discos duros, 152 CD Rom, 751 disquetes, 1 GSM, 1 monitor de ordenador y 1 talonario de cheques. El material incautado no ha sido aún devuelto, según sus dueños.

Fue la primera redada contra miembros de la comunidad hacker, que reaccionó con gran sorpresa. En los meses y años siguientes, Angeloso llevó a cabo una amplia campaña de información sobre el caso, escribió textos y más textos que se publicaron en la web y se mandaron a listas interminables de *mails*. Fue una campaña nunca vista hasta entonces en la Internet hispana, con ella provocó una corriente de simpatía hacia los acusados y en contra de la BSA y su abogado, Javier Ribas.

> Hubieron muchas irregularidades en todo el proceso y definitivamente no fue justo, fue todo un proceso de cabeza de turco, pues querían eso para asustar.[24]

La actuación de las fuerzas de la ley, ignorantes entonces sobre cómo llevar un caso de este tipo, dejó bastante que desear. Por ejemplo, explicaba la revista "iWorld", el périto habría borrado un directorio del servidor investigado y se habría llevado los ordenadores incautados a su casa, sin reportarlo correctamente.[25]

En medio del temporal, Angeloso y Maki se pelearon. En 1999, Angeloso se marchó a Estados Unidos. El juicio tardó ocho años en celebrarse, hasta junio de 2005, cuando un juez dictaba por fin sentencia. Sería la primera condena en España por difusión de cracks en Internet. Fer13, como creador de *Viva el Jamón y el Vino* y ser quien incorporaba los cracks, y Maki, como administrador y copropietario de la página, eran condenados a 2 años de prisión, el pago de 6.000 euros en concepto de daños morales a cada compañía denunciante, más una indemnización por daños y perjuicios de posiblemente 7,5 millones[26]. Dicha condena no es definitiva y el proceso sigue inconcluso, camino del Tribunal Supremo Español.

Angeloso no fue juzgado por vivir en Estados Unidos. Estuvo declarado en rebeldía procesal y paradero desconocido.

2.2. La versión de la prensa


CIBERESPACIO
¡¡ALTO, POLICÍA!
FOLLÓN LEGAL EN INTERNET
LA JUSTICIA ARRUINA UNA EMPRESA INFORMÁTICA

Reportaje publicado en la revista “Hablan”, en octubre de 1997

El caso Vestec inaugura en los medios de comunicación la tradición de tratar desde la ignorancia y el sensacionalismo todo lo que tenga que ver con el hacking, que es automáticamente criminalizado. En cambio, los cada vez más periodistas que informaban desde la red ofrecieron visiones más realistas. Como Ángel Cortés, quien desde “Noticias Intercom” se llevaba las manos a la cabeza por las declaraciones sin pies ni cabeza que estaban haciendo la policía y la BSA:

> El director general de la Policía Juan Cotino, destacaba en Málaga (según fuentes de la Agencia Efe) “la desarticulación ayer en Barcelona de una banda de cuatro individuos que falsificaban programas de ordenador a través de la red informática Internet y contaban con una red de 400.000 clientes”. Por si fuera poco, seguía explicando que “Esta organización, cuyo actividad se cifra en miles de millones de pesetas, también creaban virus en otros programas que no se podían falsificar y creaban tarjetas de crédito para poder entrar en Internet”.
>
> La propia BSA (según información recogida por la agencia Europa Press) también contribuía a la confusión, al dar a conocer la “desarticulación de la empresa VESATEC que aparentemente se dedicaba a distribuir vinos, y que contaba con más de 2.000 clientes en todo el mundo (..)Las herramientas de neutralización (de programas) se distribuían bajo la imagen de estar dando a conocer bebidas alcohólicas”. **[27]**

Otros periodistas, como el veterano Wicho, ponían las cosas en su sitio explicando como Isla Tortuga no dudaba en ganar dinero con su propia caída en desgracia:

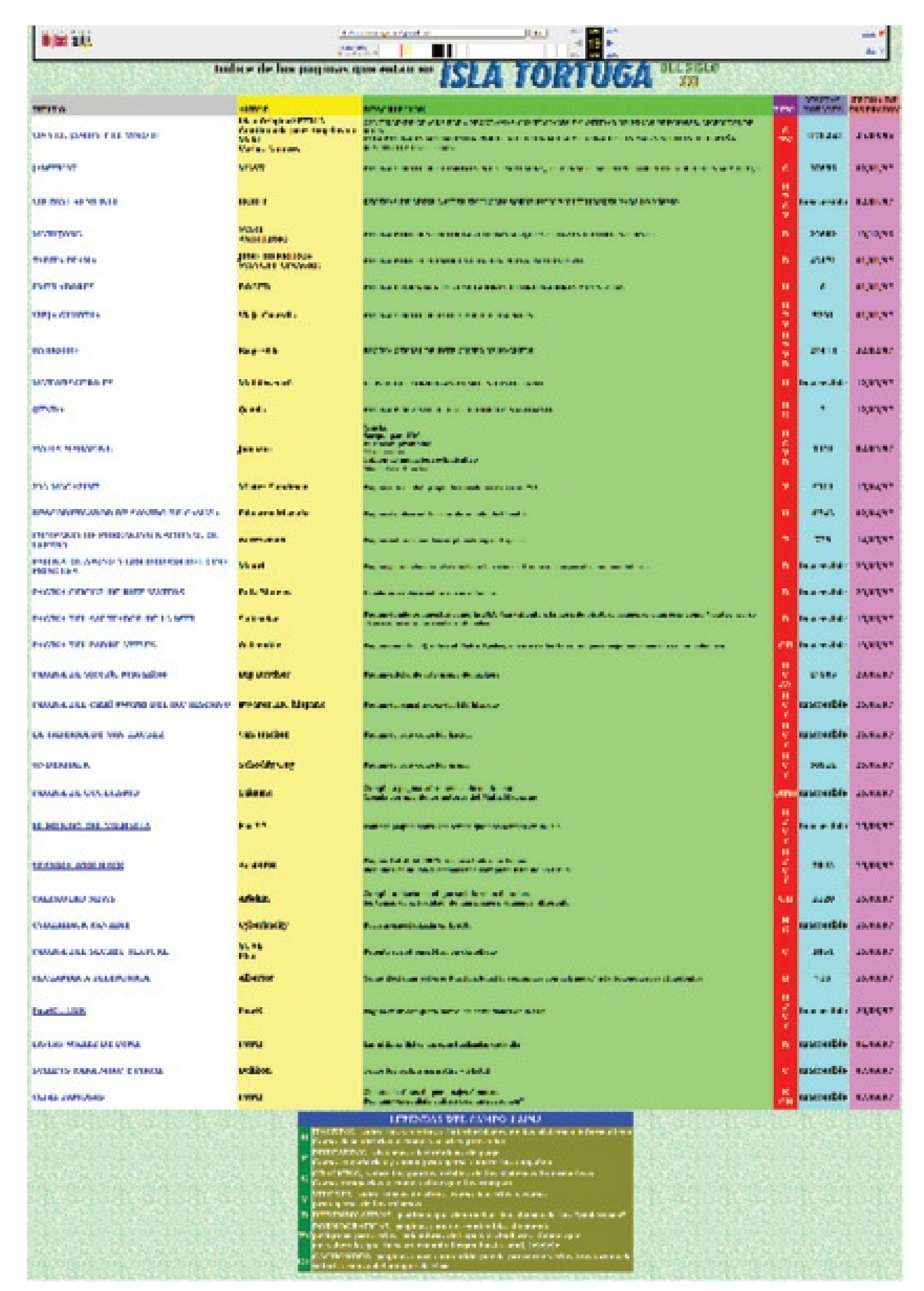
> Parece claro que por ahora los socios de Vesatec están decididos a sacar provecho de su momento de gloria, pues el mismo 13 de junio a las 10 de la mañana su servidor volvía a estar en línea, y parecen dispuestos a conseguir hacer todo el dinero que puedan en el menor tiempo posible aprovechando los miles de visitas a su web que sin duda este caso generará. Tras haber sido cerrado su servidor, Vesatec ha vuelto a la actividad con una amplia oferta de servicios Internet de todos los tipos, dispuestos a hacerse de oro.**[28]**

2.3. Consecuencias

La redada de Isla Tortuga fue un duro golpe para un “underground” acostumbrado a la impunidad. Era la primera vez que las fuerzas de la ley actuaban contra un sitio web en España, y no cualquiera: Isla Tortuga, la *casa* de la escena hacker. Los grupos que allí “vivían” vieron como sus webs desaparecían de la noche a la mañana y había que buscar un nuevo alojamiento.

Todos los habitantes de la red hispana, hackers y no hackers, vivieron con sorpresa el cierre de Isla Tortuga, que provocó multitud de comentarios en los foros y webs, muestras de solidaridad, apelaciones a la libertad de expresión y en contra del cierre de un sitio web.

Un mes después de la redada, Isla Tortuga volvía a estar en marcha, con el nombre Isla Tortuga del Siglo XXI.



Páginas hospedadas en Isla Tortuga en enero de 1998, según Internet Archive. [ampliar]

Pero la alegría duró poco. En diciembre de 1998 se cerraba la página *temporalmente*[29]. Los anunciantes habían retirado la publicidad por falta de visitas y Servitec (Servicios Avanzados en Internet SL), la empresa que había sustituido a Vesatec, estaba al borde de la quiebra, que se produjo en agosto de 1999.

3. es.comp.hackers

La comunidad hacker hispana de los 90 tenía diversos sitios para reunirse, siendo las plataformas más comunes las BBS y, en Internet, los chats, los grupos de noticias y las listas de distribución de correo electrónico. Uno de los foros más antiguos era el grupo es.comp.hackers, creado a mediados de los 90 en la jerarquía española es. de Usenet. En 1999 nació su hermano es.comp.cracks.

Según los archivos de Google Groups[30] los primeros mensajes en es.comp.hackers aparecieron en enero de 1997, aunque algunas fuentes afirman que ya existía en 1996[31]. [Ciclo natural de vida de una lista de correo] Como ya es habitual en los foros de la red], en sus inicios el grupo tenía muchos mensajes y de alto nivel técnico. Entre sus contertulios destacaban **Lokutus**, **Drizzt**, **Agustín MuNoz**, **NBK**, **Lecter**, **David Martínez**, **Crin0**, **Spinnet**, **[OMG]**, **Isocrono**, **Seldon**, **Santiago (Milon)**, **Haste** y **Vladimir**.[32]

En el año 2000, de es.comp.hackers surgió el grupo de seguridad informática Alea Hackta Est (A.H.E.), muy crítico con la situación que empezaba a vivir el foro, donde de 200 mensajes diarios, no más de 10 tenían interés y el resto era spam:

> La situación del grupo fue empeorando. Junto a los mensajes relacionados con el hacking, que cada vez eran más, también aumentaban los mensajes de provocadores, spammers, pidones, etc… hasta tal punto que resultaba casi imposible encontrar los mensajes interesantes entre tanta basura.[33]

3.1. El proyecto Hackindex

Alea Hackta Est nacía con la misión de educar en temas relativos a seguridad informática y hacking ético. Su iniciativa más ambiciosa fue HackIndex: *Un Proyecto de Dominio Público del Grupo de Noticias: es.comp.hackers*[34], que creaba y recopilaba artículos de la comunidad para servir de guía básica a los novatos y de perfeccionamiento al resto. NBK, [OMG] y CrinO los recogían en sus webs.[35]



El 8 de julio del 2000 se creaba la lista de correo HackIndex[36], como plataforma de comunicación del proyecto. La lista era moderada (por NBK y Seldon) para evitar los abusos que habían acabado con es.comp.hackers. Sólo en los primeros días se suscribieron más de 100 personas y llegó a tener 3.779 suscriptores[37]. La primera web oficial surgió también entonces: Hackindex.

Un año después, el 24 de marzo de 2001, nacía otra lista de correo, CrackIndex[38], moderada por **Marmota**, NBK y Seldon, que llegó a tener 1.570 suscriptores.

A pesar de arrastrar el calificativo de “hermana pequeña de HackIndex”, lo cierto es que es una lista de gran nivel en la que se ha reunido gente muy importante de la escena hispana, y donde están representados con uno o varios miembros todos los grupos de cracking hispanos.[39]

Hackindex contó también con un canal de chat, #hackindex, dentro de la red IRC Vulcano[40], donde se organizaban charlas.

Otro interesante proyecto de Alea Hackta Est fue la Operación SambaBios, liderada por Protocolocon, quien creó el programa *Notificador_139* que escaneaba la red a la búsqueda de ordenadores con permisos de escritura a través del protocolo NetBios, que en aquella época eran muchos pues Windows los habilitaba por defecto.[41]

Cuando el programa daba con un ordenador inseguro, mandaba una aviso al escritorio del usuario, cuya cara de sorpresa debía ser memorable. En el mensaje, se le explicaba que a través de este agujero podrían robar, borrar o manipular datos de su ordenador y cómo solucionarlo.[42]

Los miembros de Alea Hackta Est eran en su mayoría veteranos de la escena hacker y cracker: N.B.K., Seldon, Lecter, **Protocolon**, Crin0, Lokutus, Spinnet, Marmota, **El S@nto**, **Crack el destripador**, **Pist0ne**, **Kdt00ls**, **Pumucky**, **David Martínez Oliveira**, **^SirAk^** y Milon. Con el tiempo se les unirían **Alexander Upierz**, **ByTrack**, **estrella**, **ilopez**, **MrJade**, **NaG**, **protocolocon**, **Reinoso G.** y **^SiR_AK^**.[43]

3.2. Lista de correo Hacking

En el panorama de las listas de correo públicas de la comunidad hacker, la decana y pretendidamente de alto nivel fue la lista moderada Hacking. La creó Jesús Cea (jcea) a principios de 1997 y llegó a tener 1.000 suscriptores, entre ellos lo mejor de cada casa de la escena hacker hispana.

Hacking había nacido como una lista privada en la que participaban administradores de sistemas amigos de jcea, con la obligación de mandar algo interesante en un lapso de tiempo determinado (cada mes, cada dos...) so pena de ser dados de baja. Más adelante se decidió hacerla pública y eliminar la condición de tener que aportar algo para seguir en la lista. Jesús Cea describía así las motivaciones que le llevaron a crearla:

Nunca ha sido mi misión crear una comunidad virtual de hacking, cosa que veo muy difícil debido al secretismo y a la tradicional tendencia solitaria que rodea a este mundillo. Mi intención, por contra, es proporcionar un espacio neutral para intercambiar preguntas y respuestas entre personas con un nivel de conocimientos y experiencia aceptablemente altos, y hacerlo sin vincularlos a ninguna tendencia o movimiento determinado. Intercambio de información en estado puro.[44]

4. IRC-HISPANO

La red de Internet Relay Chat IRC-Hispano fue El Territorio con mayúsculas de la comunidad hacker de los 90.

Nació en 1996 de la mano de tres proveedores de acceso a Internet: EncomIX, en Zaragoza; LleidaNet y **Conexis**, en Cerdanyola del Vallès (Barcelona). Pronto se les unieron otros proveedores hasta llegar a los 24 en 2002, su época dorada, cuando era una de las 10 redes más grandes del mundo.



Los ISPs que iniciaron esta aventura acababan de nacer a finales de 1995. El más viejo era EncomIX, registrado como empresa el 1 de febrero de 1993. EncomIX era la evolución natural de la BBS del mismo nombre, que había montado Ramón Martínez en 1987. Martínez era *Ender Wiggins*, del grupo hacker Apòstols. También LleidaNet venía de una BBS y era obra de un apòstol, *The Phreaker*, Jordi Murgó en el Mundo Real. En cuanto a Conexis, su director técnico, Jordi Figueras, era amigo de Murgó.

EncomIX y LleidaNet ya estaban conectados entre sí: EncomIX tenía diversos módems en LleidaNet, para que sus clientes en Lleida pudiesen acceder a Internet con llamada local. Los servidores IRC de ambos ISP también estaban conectados, en lo que Martínez llama *el IRC de Apòstols*.

Paralelamente, un chaval que hacía prácticas en Conexis, Toni Panadès (alias *Crazy*), usuario de diversas redes internacionales de chat, propuso a su jefe, Jordi Figueras, conectar el servidor IRC de Conexis con el de LleidaNet para crear una pequeña red. Así lo hicieron y EncomIX se les unió automáticamente, al estar ya conectado con LleidaNet.

A partir de aquí surgieron nuevas ideas para esta red, aún sin nombre. Panadès contactó con el administrador de un servidor IRC de la Universidad de Aguascalientes, en México, para ampliar la red. Hicieron pruebas unos días pero el experimento no funcionó ya que el lag lo hacía imposible de gestionar.

Y así, experimentando, la red empezó a crecer: se le unieron otros ISP como **Minorisa**, de Manresa, y **Argo**, de Madrid, que aportó a uno de los mejores técnicos que ha tenido IRC-Hispano: Jesús Cea, administrador de la lista de correo Hacking entre otras aficiones. Pero el peso más pesado fueron los sevillanos del ISP **Arrakis**, capitaneados por Luis Torrado y Juan Ignacio Rodríguez Tejada, alias *Rayita* en sus tiempos de correrías con Ramón Martínez. Rayita era uno de los pocos a quienes Ender Wiggins enviaba saludos en su famoso Manual del novicio al hacking.



Arrakis había nacido en diciembre de 1995. Estaba apostando por los precios baratos y fue el primero que se anunció en televisión, por lo que tenía diez veces más usuarios que el resto de ISPs juntos. Contaba además con una red de IRC propia, de forma que se podría decir que, más que unirse al IRC-Hispano, este y la red de Arrakis se fusionaron.

> Arrakis creía mucho en su servicio de IRC, desde antes del Hispano.**[45]**

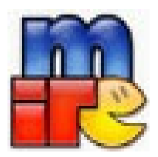
Viendo que el experimento crecía, Panadès propuso crear unas normas de funcionamiento para la red, a la que bautizó en su propuesta como *IRC-Hispano*, pensando en la posibilidad de que sitios como Aguascalientes se uniesen al proyecto. En una reunión en Lleida se aprobó el nombre y nació oficialmente la red, creada por empresas pero no comercial, como afirma el documento fundacional.

> IRC-HISPANO se define como una red de IRC no comercial, abierta a todo el mundo. IRC-HISPANO nace con la intencion de unir a la comunidad de usuarios de habla hispana.**[46]**

Y así se mantuvo hasta que se convirtió en asociación, en 1999. Como agravio histórico hay que decir que a Toni Panadès no se le dieron ni las gracias, de forma que cuando acabó su relación laboral con Conexis, en 1999, le borraron como administrador de IRC-Hispano.

4.1. La separación de Arrakis

En enero de 1998, la red tenía 2.101 usuarios, 693 canales, 5 operadores y 22 servidores y su crecimiento, como el de toda Internet, empezaba a ser exponencial. En octubre de 1999, el canal #marketing, liderado por Mar Monsoriu, llevaba a cabo la primera encuesta sobre quiénes eran aquellos “chateros”: hombres, solteros y universitarios.



> Hombre (75,9 %) de nivel universitario o superior (doctorado o master) que vive en una ciudad, lleva varios años en Internet, se conecta desde casa (en un 60 %), es soltero pero no vive solo (77,6 %) y tiene un poder adquisitivo que le permite pagar una factura telefónica de 40.000 pesetas.**[47]**



La escena hacker hispana, hasta entonces desperdigada por otras redes como EFnet o Undernet se mudó en masa al Hispano. Se abrieron canales míticos que

estarían llenos cada noche durante años, como #hack, #hackers, #phreak, #hpcv, #hackademia, #virus, #hack_novatos.... y otros con nombres menos explícitos pero también territorio de algunos buenas piezas, como el #barcelona**[48]**.



Los mejores hackers del país se volcaron en hacer funcionar la red. Alli estaban Ender Wiggins y The Phreaker, ahora *Rampa* y *Savage*; Rodríguez Tejada desde Arrakis; Jcea, con la gorra del ISP Argo, programando a Nick2, Agenda, Chan2, Chanfollower, Lazoazul o Argobot. Pronto vendrían otros, como Luis Monedo (alias *Somatic*), creador de la comunidad virtual #Ayuda_IRC.



Posiblemente, todo habría ido como una seda si sólo la élite -la auténtica élite- hubiese metido mano en IRC-Hispano. Pero las cosas nunca funcionan de la forma ideal que sueñan los técnicos y pronto empezaron los problemas terrenales y humanos, las rencillas, los "mi proveedor es mejor que el tuyo", los "quiero mi dinero", los *marketroides*, los adictos al chat, el poder que emborracha y, sobre todo, el Ego, el super-ego de los hackers.

La que sigue es la descripción de una guerra entre viejos hackers por la conquista de un territorio en el ciberespacio llamado IRC-Hispano. Algunos la han llamado la guerra de Arrakis contra LleidaNet y viceversa. Otros, de cuando el Hispano se partió en dos. Y también, la caída de Goku. En todo caso, es una historia oscura donde no se tuvo en cuenta el lema de la ética hacker, *la información quiere ser libre*, pues nadie explicó nunca toda la verdad, que se escatimó al público. Una frase del periodista Pedro de Alzaga resume con certeza el por qué de aquella guerra:

> Aunque la iniciativa fue un éxito absoluto entre los internautas, su desarrollo ha estado plagado de problemas entre sus administradores.**[49]**

4.1.1. Goku y Scytale

En 1999, CTV, RedesTB, Servicom y Ergos entre otros se habían unido también al IRC-Hispano. Pero Arrakis seguía siendo más grande que todos juntos: a finales de 1999 una auditoría reveló que el ISP tenía 40.000 usuarios directos, cifra más que respetable. El 70% de personas que entraban al IRC-Hispano venían de Arrakis y el canal #sevilla (ciudad donde se ubicaba el ISP) era el más poblado. Arrakis era

también el proveedor que aportaba más servidores a la red: seis. Un monstruo que no gustaba a todo el mundo, pues reclamaba una cuota de poder proporcional a lo que aportaba.

Rodríguez Tejada y un amigo, Alberto Rodríguez Ortega, subdirector técnico de Arrakis, que respondía al apodo *Goku*, habían adaptado y reescrito un robot o *bot* de mantenimiento de redes IRC[50], al que llamaron Scytale[51][52] y que se convirtió en el robot oficial del IRC-Hispano, junto con el que había funcionado hasta entonces en solitario, Argobot.

Goku se encargó de administrar a Scytale y después de un tiempo cohabitando, Argobot fue apartado de mala manera[53], explica Jesús Cea:

> Súbitamente y sin previo aviso, Arrakis introdujo su bot Scytale y expulsó a Argobot de la red.[54]

La versión de Rodríguez Tejada es otra:

> Es posible que el argobot llegara a funcionar cuando Argo estaba haciendo pruebas antes de formar el irc-hispano que conocimos, yo no llegué a verlo, por eso se creó Scytale porque no teníamos nada.[55]

Sea como sea, en aquel momento nadie alzó la voz pues, como explica Murgó[56], la red necesitaba que alguien pusiese orden y se encargase de ella. Hasta aquel momento, Hispano había sido un mundo desorganizado, donde se daban privilegios de IRCop al tun tun. Goku y Scytale venían a poner límites. Lo explica también Rodríguez Tejada:

> Nadie designó a nadie, irc-hispano no tenía ninguna clase de dirección o forma de gobierno ninguna, simplemente en Arrakis nos preocupábamos por lo que pasaba y tuvimos que tomar las riendas cuando las cosas empezaron a desmadrarse. Ya sabes, la gente peleando por los canales, usando bot de combate y cosas de esas. Como nadie hacía nada práctico, y solo discutían sobre las forma de hacer las cosas y no se decidía ningun plan de acción, nosotros reaccionamos y tomamos el control de la situación.[57]

Pero se les fue la mano. Goku convirtió el Hispano en su cortijo, donde hacía y deshacía con la aquiescencia por desidia del resto de ISPs. No había usuario que no odiase a Goku. Criticaban su comportamiento dictatorial a la hora de resolver los asuntos de la red, ejerciendo un control total de la misma y otorgando privilegios a sus amigos frente al resto de usuarios, así como a Arrakis frente al resto de proveedores. En la página de *Tranx*, un histórico del canal #barcelona, detenido en 1997 por hacking a la Universitat Rovira i Virgili, puede leerse una muestra del odio que los usuarios le tenían:

> Chepa-IRCOPS (Recopilacion de los IRCOPS que putean al projimo): Son los que van de Texas Rangers con su lema “To serve & Protect”, se les ha subido a la cabeza lo de ser IRC-OP y se creen superiores, cuando en realidad son unos crios que necesitan 2 sillas pa sentarse. Esta tribu la componen: Goku, Lightman, Elcuervo, Gard, {^NoGuE^}, Jany (defensor de Culturist-BINARIA-Rambo).[58]

Todo un antihéroe. Una década después aún se recuerda a Goku y se cuentan historias que rayan la leyenda urbana. Esta situación acabó creando muy mal

ambiente, como se explica en la *Historia del IRC-Hispano*:

> Ante la oposición de la mayoría de servidores se vive una etapa tirante, en la que Arrakis crea los CServices**[59]**, que sustituirían desde ese momento a los IRCops. La total oposición por parte de los ISP fundadores permite plantear nuevas alternativas para evitar el monopolio.**[60]**

4.1.2. Los dos Hispanos

Goku se había convertido en el rey del Hispano y nadie le amenazaba. ¿Nadie? Una niebla confusa sigue cubriendo qué pasó realmente. Cada cuál contó su versión y ninguna era muy clara, quizás porque detrás había, por parte de ambos bandos, intenciones dobles y mentiras.

Todo empezó, según denunció Arrakis en un comunicado**[61]**, porque el resto de proveedores de IRC-Hispano crearon una red paralela. Sisco Sapena, de LleidaNet, confirmó a "El Mundo"**[62]** la creación de esta red, pero aseguró que Arrakis estaba informado. Entre líneas podía leerse que querían dejar a Goku sin "juguete" y a Arrakis sin el control del Hispano.

La versión de Jordi Murgó, autor de los robots que acabarían sustituyendo a Scytale, es otra: Murgó y unos amigos, entre ellos los hackers portugueses ToXyN, tenían una red de IRC privada, DarkNet. Murgó había creado tres bots con los que estaba experimentando: *Nick*, *CHaN* y *MeMO*, que eran una adaptación de los bots de la red de IRC DalNet, creados por Andrew Church. Chan controlaba canales y usuarios. Memo administraba el sistema de mensajería y Nick, el registro de *nicks*.

> Invité a algunos administradores a la red para que pudiesen probar las mejoras que estaba implementando en ella. Uno fue Goku, quien se asustó cuando vio los bots, le entró la paranoia de que queríamos ponerlos en el Hispano y robarle el poder, cuando esta no era para nada la intención. Y, a partir de aquí, actuó presa del pánico.**[63]**

Arrakis se adelantó a los que consideró preparativos para un golpe de estado: el 9 de diciembre de 1999 registró el dominio **irc-hispano.net** y, sin notificarlo a la red, empezó a preparar su marcha. Según explicó Sisco Sapena a "El Mundo", el resto de proveedores se enteraron unas horas antes de que Arrakis se desconectase del Hispano.

> "Llevamos 60 horas sin dormir". Con estas palabras, Sisco Sapena, gerente de Lleida.net y uno de los administradores del nuevo Irc hispano, resume la salida de Arrakis de la red de Irc. Según Sapena, el 31 de diciembre, y con un margen de ocho horas, un "tercero" les avisó de que el proveedor sevillano pensaba retirarse de Irc-hispano.**[64]**

Arrakis se llevaba a Scytale, lo que en la práctica significaba llevarse los canales y los nicks de los usuarios. En resumen, las ciudades y sus habitantes: la red entera. Entonces, entraron en escena los robots de Murgó, que se pasaron a producción en plan bestia, en tiempo real y con miles de usuarios pidiendo registrar de nuevo sus nicks.

Arrakis denunció que esta puesta en escena no tenía nada de espontáneo, sino que se había estado trabajando en ella durante meses y de forma oculta,

provocando problemas en la red “vieja” para que, cuando saliese la “nueva”, los usuarios la prefiriesen, y usando malas prácticas, como los netsplits, para robar nicks, contraseñas y otros datos que atesoraba Scytale.

> Eso no son formas…**[65]**

Las espadas estaban muy en alto, cada bando mostrando por fin sus cartas. De la noche a la mañana hubo dos redes con el mismo nombre: **IRC-Hispano.Net** frente a **IRC-Hispano.Org**.

4.1.3. Y ahora kasemos?

Los damnificados fueron los usuarios, quienes de repente se encontraron con que los canales que solían frecuentar estaban duplicados, en dos redes de IRC antagónicas. ¿Cuál escoger? Muchas comunidades se dividieron, yendo algunos de los habituales a IRC-Hispano.net y los otros, a IRC-Hispano.org. Para colmo, hubo una falta total de transparencia sobre qué había pasado en las alturas de los super hackers. José Francisco Coloma lo explica referido a un caso particular: el canal #alicante:

> Los usuarios del #Alicante se quedaron sorprendidos (al igual que todos los usuarios del antiguo Irc-Hispano) por la separación del Irc-Hispano. Ningún usuario en toda la red fue avisado de lo que iba a ocurrir. Y desde luego nunca se dio una explicación “oficial” y “verdadera”.
>
> Krad se reunió con el equipo de admins y por mayoría eligieron quedarse en el #Alicante del Irc-Hispano.org. Así que Krad y los suyos entraron en el #Alicante del Irc-Hispano.NET (“El otro hispano” o “El hispano de arrakis”, como decían algunos) y dejaron el siguiente topic: “Si quieres volver a ver a tus amigos del #alicante, tienes que irte a la otra red, el Irc-hispano.org. Nunca más entres a la red de Arrakis”.
>
> Todo siguió más o menos tranquilo. El #Alicante del Irc-Hispano.org se registró de nuevo con el bot Chan. A los usuarios había que explicarles el funcionamiento de los nuevos bots en directo en el chat.**[66]**

Coloma aclara más adelante, en Historia del #Alicante, que finalmente hubo un canal #alicante en cada red.

4.1.4. Las otras versiones

IRC-Hispano.net dejó pronto de existir. Unos días después de la separación, el 30 de enero de 1999, se hacía oficial la venta de Arrakis a British Telecom**[67]**.

Esto aporta dudas a la historia oficial sobre la separación: ¿Eran los dueños de Arrakis quienes querían “quedarse” el IRC-Hispano, o era British Telecom? ¿O era LleidaNet quien quería el control que se había dejado arrebatar? El director ejecutivo de LleidaNet, Sisco Sapena, quería convertir el Hispano en una asociación y aprovechar comercialmente el “boom” de usuarios. ¿Hasta dónde gustaba esto a Arrakis? ¿Hasta dónde estorbaban los sevillanos? ¿Quién traicionó a quién? ¿Y por qué falló tan estrepitosamente la comunicación? ¿De dónde salió tanta mala

sangre que todos jugaron sucio, no avisando el uno de que se iba, tramando los otros cambios vitales?

Se dice que el talante de Goku tuvo la culpa: un auténtico Bastard Operator From Hell de 20 años que, según sus pocos defensores, tenía que hacerse el duro para lidiar con las mil historias cotidianas de una red de chats, que si este me ha robado el canal, que si el otro quiere registrar un nick que también quiero registrar yo. Según otros, mayoría, Goku era un chaval borracho de poder que había llevado la situación a un punto insostenible... Pero, ¿de verdad todo este lío, de no hablarse, de robarse cosas, de guerras, por no atreverse a echar a un chaval de 20 años?

Alguien que trabajaba en LleidaNet desde que se fundó, Ignasi Cavero, alias *Glog*, aporta un potente foco de luz hacia la verdad:

> Desde LleidaNet con el apoyo de otros miembros (Encomix, Argo...) se trabajaba en tener unos bots (Nick, CHaN y MeMO) en condiciones adaptados al ircd de irc-hispano. Hacía mucho tiempo que Jordi trabajaba casi exclusivamente en adaptar los bots, pero aún eran muy inestables. Jovi, aprovechando sus privilegios de acceso a Scytale, nos 'dumpeaba' información (nicks, canales, etc), para que los pudiésemos inserir en los nuevos servicios y así, en el momento de hacer el cambio, aquello fuese lo menos traumático posible para los usuarios. Recuerdo horas y horas programando scripts para hacer aquellas importaciones de datos.
>
> Arrakis sabía que la nueva red existía, pero creo que no se le dejaron nunca claros los motivos de su existencia. Cuando le vio las orejas al lobo, y aprovechando que nosotros aún no lo teníamos todo preparado, fue cuando expulsó al resto de nodos. A partir de aquel momento todo fue correr y poner en servicio a irc-hispano.org con los nuevos servicios. El dominio irc-hispano.org era de LleidaNet, así que a Arrakis no le quedó más remedio que registrar irc-hispano.net para su red, aunque intentó quedarse el dominio irc-hispano.org.
>
> Antes de la separación nunca se 'atacó' o perjudicó a la red provocando netsplits o cualquier otra cosa. Nosotros queríamos una red que funcionase, sin Arrakis como Dios todo poderoso. De hecho, la intención era EXPULSAR a Arrakis.
>
> Arrakis precipitó con su actuación unos acontecimientos que se habrían llevado a cabo poco después, en cuanto lo tuviésemos todo preparado.**[68]**

Murgó matiza:

> No recuerdo que fuera algo tan planificado, y creo que esos dumps de nombre de canal se hicieron al saber q se irían. Para mi, como para jcea y glog, el único interés fue siempre el reto tecnológico.**[69]**

Es esclarecedor atisbar cómo siguió la historia: a partir de la marcha de Arrakis, la red se convirtió en un ente comercial y comerciable, algo con lo que no todos, empezando por su inventor Toni Panadès, estuvieron de acuerdo.

> Desde mi punto de vista de actor en la sombra, el proyecto IRC-Hispano fue desviado de su propósito inicial, aunque lo comprendo dada la importancia que rápidamente cobró. A partir del momento en que Lleidanet impulsa la asociación y toma el control, se convierte en una herramienta de promoción para los nodos que forman parte del mismo.**[70]**

4.2. Money money

En julio de 1999, en una reunión en Lleida, se creó la asociación del IRC-Hispano, como *"asociación privada de ámbito nacional, sin ánimo de lucro"*[71], y Sapena fue designado presidente, un cargo que ostentaría hasta 2007[72][73], cuando el Hispano ya estaba en decadencia.

Sapena aportó seriedad a la red y un gran interés en conseguir lo que él llamaba su "independencia económica", lo que convirtió la gestión de Sapena en un experimento único en el mundo: cómo hacer dinero con el IRC.

> Los proveedores de IRC-Hispano sacaban un provecho claro que era el servicio más barato que podían ofrecer: el IRC, y a cambio tenían muchos usuarios conectados mucho tiempo.[74]

Por la red no sólo viajaba tráfico IRC sino también correo y otros servicios, lo que abarataba los costes[75] de los proveedores, que aportaban los servidores de la red y una cuota mensual de 5.000 pesetas (30 euros).

Pero creían que podía sacarse más de aquella monstruosa comunidad que no paraba de crecer. Y con tanta gente mirando, una de las primeras cosas que se les ocurrió fue la publicidad. Así, el 22 de septiembre de 1999[76] el Hispano montaba un estand en la feria SIMO, donde ofrecía originales ideas a las empresas, como anunciarse en los canales más poblados de la red usando robots.

Pero, antes de poner en marcha su plan comercial, la asociación tenía que "limpiar" el Hispano, darle una imagen de sitio seguro para el capital, así que empezó cerrando algunos canales incómodos, como el histórico #cannabis, en mayo de 1999[77][78].



Cartel de protesta por el cierre del canal #cannabis y otros en IRC-Hispano

El segundo paso fue abrir el Hispano a las fuerzas de la ley. Desde la época de Arrakis la red investigaba y denunciaba de forma discreta situaciones irregulares, como la pedofilia. Después de Arrakis, Hispano no sólo ayudaba a los policías en sus investigaciones, sino que a partir de verano del 2000 también les ofreció cursos de formación.

Y empezaron a sucederse las noticias de redadas a partir de investigaciones iniciadas en el Hispano[79][80][81]

> En el último año, la asociación ha hecho más de cien denuncias por pedofilia y cincuenta por anuncios de pornografía en canales de menores. “Tenemos un grupo de voluntarios dedicados a la búsqueda y captura de esta gente. En abril se hizo la primera redada, con dieciocho detenidos”, explica Sapena.[82]

Pero limpiar el IRC-Hispano no era fácil, pues la red empezaba a ser un ente más que respetable: en agosto de 1999, tiene 44.000 nicks registrados, 3.000 canales y medio millón de visitantes diarios, y sigue subiendo a un ritmo vigoroso. Según Sapena, se triplicará esta cifra en menos de un año.[83]

La autofinanciación es la única forma de soportar tal avalancha, afirma Sapena[84].

Entre sus propuestas para comercializar el Hispano hay originales ideas: canales esponsorizados por empresas; robots vendiendo entradas, o billetes, o actualizaciones de juegos; mensajes globales a todos los usuarios conectados al Hispano...

Algunas se ponen en marcha, pero lo que funciona mejor son cosas menos originales, como cobrar a los proveedores por formar parte del Hispano, cobrar a los cibercafés el derecho a tener clientes conectados a la red, y el registro de canales (relacionado con NoExpire, lo hablamos más adelante).

Mientras, aquel mismo año 1999, cuando Hispano vivía su gran momento de éxito, dos de sus fundadores se iban: Toni Panadès y Ramón Martínez, quien vendió su ISP EncomIX a la empresa estadounidense PSINet[85]. No tardaría en irse Jordi Murgó, el 1 de julio de 2000, por desavenencias con Sisco Sapena.

Y volvió Arrakis, ahora bajo la dirección de British Telecom.[86]

4.3. Trifulca va, trifulca viene

Algo que caracteriza a toda red de chats y el Hispano no fue una excepción son las discusiones y luchas, tanto en las alturas de los *dioses*: las empresas y los IRCops; como en el terrenal mundo de los usuarios y sus héroes, aquellos hackers que jugaban con sus scripts a la guerra en el IRC:

> El IRC-War consistía básicamente en diferentes mecanismos para poder cortar las conexiones a Internet de tus enemigos virtuales mediante exploits, nukes o ataques de flood (...) puesto que los piques en el chat eran frecuentes. (...) Probablemente el script que empezó esta moda fuese el 7th Sphere ya que venía equipado con una serie de programas ejecutables que automatizaban la mayoría de los ataques más frecuentes.[87]

Y aquellas peleas por ser *operador*:

> Dentro de la 'sociedad del IRC' había diferentes jerarquías. Los operadores de canal tenían una arroba delante del nombre y podían echar a la gente. Así surgió un juego de poder en el que tenías que ser amigo de los operadores para que te diesen @ y así ser de los que mandaban. La más interesante era la @ en el canal de tu ciudad, en el que estaban las chicas que te interesaban.[88]

De las luchas en el IRC, que forjaron a los hackers especialistas en defensa y ataque, son buen testimonio documentos como las famosas Tácticas de guerra en el IRC que escribió *Román Medina-Heigl Hernández* (RoMaNSoFt). La primera versión apareció en 1997[89] y la última en 1999[90].

> No tengo un "medidor de difusión" pero creo que fue bastante amplia, se encontraba en la sección de documentos de muchísimas webs de hack. También es cierto que el IRC estaba entonces en su apogeo y que la seguridad se encontraba en un estado muy precario, por lo que daba mucho juego a los hackers (o aprendices de), sin necesidad de ser ningún genio. Las comunicaciones también eran frágiles. Recuerdo que gente desconocida me abría queries en plan "eres el autor del documento de tacticas?" o que me invitaban a sus canales.[91]

RomanSoft no pertenecía a ningún grupo de hackers del IRC, sino a uno de los mejores grupos españoles de aficionados al Commodore Amiga: **LLFB**.

Pero había que ir con cuidado de a quien se ofendía, pues la venganza podía ir mucho más allá. Fue el caso del coruñés Santi Garrido, alias *Ronnie*. Tenía 24 años cuando los IRCops le expulsaron de la red por una discusión. Ronnie se dedicó entonces a infectar con un virus-gusano llamado *Deloder* a un ejército de miles de ordenadores en Europa y Asia. El gusano convertía a los ordenadores en "zombis" a sus órdenes, y Ronnie los lanzó contra el Hispano... en ataques por sorpresa durante nueve meses, hasta mayo de 2003.**[92]**

Cuando fue detenido, Ronnie aceptó los hechos y se llegó a un acuerdo: dos años de prisión, multa de 3.240 euros e indemnización de 1.384.459 para Wanadoo, LleidaNet, Ono y la Asociación IRC-Hispano. Era la primera sentencia por un ataque de Denegación de Servicio en España y se la consideró "ejemplar", pues sólo otra anterior relacionada con la informática había conllevado pena de cárcel: la de un catalán condenado a tres años en 2002 por copiar la base de datos de su empresa.

5. La Vieja Guardia

Muchos grupos de hackers son hijos del IRC, empezando por !Hispahack. Pero ninguno con la solera de La Vieja Guardia que como !H, del que era la cantera, tenía su propio canal: *#hpcv*. La Vieja Guardia nació a finales de 1996 en el IRC de Arrakis y desapareció en 1999.

Empezó como un foro dedicado a la investigación en seguridad informática, redes y telefonía. Su líder fue **Case Zer0** y el resto de integrantes: **DarkNail**, **MainBoard**, **Mr. White** (creador de Whiskey kon Tekila), **BillSucks**, **Binaria** (una de las pocas mujeres que se movían en estos ambientes), **TaNiS**, **fit0**, **DarkCode**, **Wotan** y **Jany**.

> Nos dedicábamos a obtener control sobre todos los sistemas que podíamos, pues entonces no había el acceso a la tecnología que hay ahora y era muy difícil poder jugar con routers Cisco, redes grandes, sistemas x25, por lo que cualquier IP siempre tenía un mundo para jugar detrás y pasar horas. **[93]**

Tenían un sitio web en Geocities del que Internet Archive conserva algunas páginas: http://web.archive.org/web/19990222092249/http://www.geocities.com/SiliconValley

El grupo se disolvió en 1999. TaNiS se unió a !Hispahack. El resto se reconvirtió en Total Core Dump y Kernelpanik.

5.1. El bug del Out of Band (OOB)

El descubrimiento más destacado -aunque discutido- de La Vieja Guardia fue el *bug del OOB (Out of Band)* o cómo provocar a través del IRC la llamada Pantalla Azul de la Muerte (Blue Screen of Death): cuando el sistema operativo Windows detecta un error grave del sistema, la pantalla se pone de color azul y todo se bloquea. BillSucks descubrió cómo provocar estos errores a voluntad, mandando un paquete de “fuera de banda” (Out Of Band) al puerto 139 del ordenador, y lo automatizó con el programa *Muerte.exe*, documentado en fecha 16-04-97.**[94]**

> Respecto al OOB, se descubrió cuando desarrollaba una utilidad para el lugar donde trabajaba entonces... lo cual no quiere decir que algo similar circulara por otros servidores de IRC.**[95]**

Lo cuenta también TaNiS:

> Lo encontramos cuando Billsucks hizo un escaner de puertos y, haciendo pruebas contra la gente del IRC, vimos que cuando escaneábamos los puertos 134 a 139, dedicados al RPC, la gente se caía. Recuerdo esa tarde y lo bien que lo pasamos. Nos dedicamos unos días a hacer el animal, jugando con los servidores de Microsoft y las grandes multinacionales, porque entonces no había muchos cortafuegos.**[96]**

El reporte público de este agujero apareció unos días después, el 9 de mayo de 1997**[97]**, en la lista de seguridad informática Bugtraq, pero no lo mandó La Vieja Guardia, lo que ha provocado polémica sobre la autenticidad del descubrimiento. Diversos medios informaron sobre el mismo, incluido el “New York Times”. Pronto se automatizó este ataque con los programas llamados WinNuke**[98]**, que dieron horas y horas de diversión a los bromistas y vándalos del IRC.

5.2. Reyes del IRC

La Vieja Guardia es claro representante de los grupos que aparecen en la segunda mitad de los 90 y cuyo sitio natural de reunión ya no son las BBS sino el IRC. Al haber más gente en Internet el número de grupos de hackers era también mayor, aunque su ciclo de vida era menor.

Los canales *#hack*, *#hackers*, *#phreak*, *#virus*, *#hackademia* o *#hack_novatos* tenían al menos un grupo que los controlaba, además de gente de otros grupos que los visitaba con regularidad. Undersec, por ejemplo, solía reunirse en los canales *#netsearch* y *#hack_novatos*. No eran sus canales oficiales, pero todos los integrantes del grupo tenían *op* allí. Lo mismo puede decirse de La Vieja Guardia, que tenía canal propio en #hpcv y se pasaba la vida en el #hack. O Green Legend y otros de SET, asiduos al canal #phreak. En el canal #hackers pululaba un fugaz grupo, Wakanda, nacido en 1997 y que en su web mandaba saludos a medio "under":

> Desde aquí enviamos un SALUDO a toda la peña del canal #hackers del irc-hispano.org (ya sabeis, toda esa carroña de servers con nombres de planetas) Saludamos especialmente a: ^ViRuS^, MuErTe, Koji, SagE, aRUs997, KoNtRoL, [Chanur], Fragel, MoLly, ufo, RiDdLe, Hackelin, TheWizard, Nobody, Vandals ...etc Y En Especial a Todos los miembros de @p0kalypSYS, JJF HACKERS TEAM y UNIVERSE HACKED Si nos olvidamos a alguien que nos perdone. ;-)**[99]**

Existían también canales privados en los que se requería contraseña para acceder. Allí circulaba información de mayor calidad, como errores descubiertos en sistemas aún no reportados de forma pública:

> Solo se entraba bajo estricta invitación y circulaban muchos bugs no publicados, bien por que carecian de utilidad, o bien porque querían seguir usándose un tiempo antes de que saltaran las alarmas. (Hoy) siguen existiendo sitios de reunion similares para compartir exploits antes de ser publicados.**[100]**

Los integrantes de estos grupos, públicos y privados, respondían a la nueva definición que en aquellos momentos tomaba la palabra hacker: ya no significaba en global un experto en redes y ordenadores o un programador, sino que el hacker y el hacking se circunscribían al ámbito de la seguridad informática: a mediados de los 90, la diversión estaba en descubrir agujeros para ir más allá. Y poder explicárselo a alguien. Pues así se construye la reputación del hacker y de su grupo.

5.3. Elitismo

Característica de esta generación, sumida en el IRC noche tras noche, fue no sólo usar el lenguaje élite para crear sus nicks, sino también su elitismo y desprecio hacia el inferior en conocimiento o el que no era de su misma "tribu". Estos hackers ya no publican la información para que otros aprendan, sino para aumentar su estatus. Tan elevada importancia personal se refleja en el egocentrismo exacerbado de algunos individuos y grupos, borrachos del Poder informático.

Egocentrismo que les llevaba a enzarzarse en disputas verbales y/o sangrantes cíber-peleas. Ejemplo máximo sería la guerra que protagonizaron, en los años 80, los grupos norteamericanos Legion of Doom (donde militaba el famoso hacker The Mentor, autor de El Manifiesto del Hacker) y Masters of Deception. Guerra que acabó con la detención de casi todos (y más gente) por parte del Federal Bureau of Investigation, en el famoso Hacker Crackdown descrito por Bruce Sterling. En menor medida y en España podría ponerse como ejemplo la guerra que en sus últimos tiempos vivieron SET e !Hispahack.

Este ambiente "bélico", de agresividad y asalto al débil, estaba siempre presente en los canales de hacking. Testimonio de ello es el famoso documento que escribió en 1997 **RomanSoft**, Tácticas de guerra en el IRC, donde se explicaba cómo hacerse con el control de un canal o entrar en los ordenadores de quienes estaban conectados al chat. Para realizar automáticamente estas funciones existían programas, llamados *scripts de guerra*, que todo buen hacker debía utilizar, además de saber securizar su ordenador para no caer víctima de los scripts de los demás.

> Recuerdo algo de ese tema, finales de la época de la llamada irc-war. Cada persona necesitaba estar al día de los parches que necesitaba, y si te pasaba algo decían que era culpa tuya por no haber parcheado.**[101]**

Aparecieron también los robots-hacker, que actuaban en las redes IRC a la búsqueda de agujeros de seguridad en los ordenadores de quienes entraban. El IRC Hispano fue territorio del robot NoSFeR:

> Lo de que cuando entrases en el IRC un bot (nosfer se llamaba) te escanease, te hundiese si tenias windows, te robase los passwords si tenias linux mal configurado, etc. era cosa de la red de IRC apostols+toxyn. Luego, recuerdo lanzar nosfer en EFNet (#linux), lo que me costó un Ban para siempre de EFnet y un ban de meses y meses de la IP de la red que administraba en EFNet. Y total por nada, entrar nosfer en un canal de #linux y empezar a escribir en el canal los passwords de root de la gente que habia allí.**[102]**

Los grupos del IRC se caracterizaban también por ser menos oscuros que sus predecesores. Tenían la posibilidad de crear sus propios servidores IRC, lejos de las grandes redes, o de cerrar sus canales y permitir acceso sólo por invitación, pero la mayoría preferían ser y estar abiertos.

Eran habituales las "kedadas" entre sus miembros, siguiendo la tradición del IRC. Hablar cada noche unía como el mejor pegamento y eran habituales las bromas y los momentos jocosos, como aquél que se hizo pasar por una chica y enamoró a tres, o la llamada de ODO al programa "Hablar por Hablar": **Odo** estaba en el canal #hackers del IRC-Hispano una noche de 1999, cuando llamó al programa de radio de la Cadena SER "Hablar por hablar" y explicó que era un peligroso hacker. Tuvo 9 minutos a la locutora en vilo, mientras le contaba -y ella le creía- que era fácil desviar cohetes de la NASA o que sus amigos habían manipulado el código del sistema operativo Windows 98.

5.4. Undersec

Otro conocido grupo del IRC fue Undersec Security Team, desde 1998. Sus miembros iniciales fueron **Freed0m**, Ulandron, **P0th**, |QuasaR|, **sturm**, PaRaNoiK, **Show**, Sp4rK, **Bruj0**, |CoDeX| y RaiSe. En 2001 se les unirían |Balrog|, HardCode, **Cafo** y **Pope**.



Undersec fue un grupo muy prolífico, tanto en la creación de herramientas como de documentación y avisos de seguridad. Además, algunos de sus miembros escribían en la revista Netsearch, nacida en 1999 del canal de chat del IRC-Hispano *#netsearch*, donde solían reunirse los integrantes de Undersec.



Kedada en Madrid. De izquiera a derecha: |QuasaR| y |CoDeX| de Undersec, Crash, Zhodiac (Hispahack), Wintermute (29A). uCaLu (Undersec) hace la foto, Sp4rk (Undersec) en primerísimo plano casi no se ve. Más tarde llegarían Doing, Homs y Nuno Treez



De izquiera a derecha: Wintermute, uCaLu y Pope

En 1999 QuasaR, uno de los nombres clave de UnderSec, escribió un interesante texto que reproducimos por su valor sociológico, pues narra cómo y por qué un hacker solitario de los 90 acaba uniéndose a un grupo:

> Luchas para que todo el mundo adquiera conocimientos. Y contestas todas las preguntas que puedes y mas. Sin embargo el tiempo pasa. Y ya son cientos de veces las que has repetido las mismas respuestas. Y casi no tienes tiempo para ti. (...) Ya estas cansado de contestar lo mismo. Y encima ves como la informacion que has dado se utiliza para fines cochambrosos. Y te das cuenta que no todo el mundo tiene lo que tu llevas dentro. No es igual. Para ti es una pasion, una manera de verlo todo. Unos retos muy muy personales. Para el resto no es mas que una manera de vacilar, de conseguir ser superior al resto.
> No, no se trata de eso.
>
> Y cuando te crees que estas solo, y que has llegado a un punto donde el callejon se cierra, das un paso mas adelante en tu camino personal y conoces a gente que se encuentra en el mismo punto del camino que tu. Y comienzas a hablar con ellos. Te entienden, les entiendes y todos tenemos objetivos comunes. Es entonces cuando se forma un grupo estable donde gente de diferentes puntos geograficos se unen por algo en comun y se establece una amistad bastante fuerte. Y asi es como se entra en la idea de formar un grupo. Un grupo donde todos juntos y bajo un nombre persigan objetivos identicos. Y
> ahora tus esfuerzos van destinados a ese grupo. Y con la gente de fuera casi que no te apetece hablar de tu tema preferido. Aun asi hay que hacer un poco de esfuerzo y dedicarle un minimo de tiempo a ellos. Porke luego, a largo plazo, se recoge todo lo sembrado. Y por eso, el grupo debe de escribir para todos. Esa es mi filosofia para el grupo y para los demas.
> Todo sea por la libertad..............**[103]**

6. Notas

1. ↑ The Jargon File, version 4.4.8
2. ↑ hacker ethic. Jargon File
3. ↑ ¿Sabes cibercomunicarte?. Mercè Molist para “Ciberpaís” (08-03-06)
4. ↑ El contexto social de la comunidad de código abierto. Resumen de la Catedral y el Bazar. Cancerbero (25-02-05)
5. ↑ The Tao of IETF - A Novice‘s Guide to the Internet Engineering Task Force. RFC 4677
6. ↑ La zona temporalmente autónoma. Hakim Bey. Trad. de Guadalupe Sordo
7. ↑ Call for Performances. Undercon 6. *2002*
8. ↑ Invitación UnderCon III (La Definitiva)
9. ↑ Especial Undercon. SET (02-11-97)
10. ↑ Conclusiones de la UC97. SET. Edición Especial Undercon’97
11. ↑ UNDERCON 0x02 (1998)
12. ↑ Invitación UnderCon II
13. ↑ Crónica oficial Undercon 98
14. ↑ Narracion de la UnderCon ‘98 por Ripper
15. ↑ Narracion de la UnderCon ‘98 por Ripper
16. ↑ UNDERCON 0x03 (1999)
17. ↑ Crónica oficial UnderCon III. The Dark Raver
18. ↑ Crónica oficial UnderCon III. The Dark Raver
19. ↑ UNDERCON III : El hack hispano se reune. GreeN LegenD. SET 21 (11-11-99)
20. ↑ UNDERCON 0x04 (2000)
21. ↑ Undercon’2000: Puro código. Scaramouche. Kriptópolis (17/10/00)
22. ↑ UNDERCON 0x08 (2004)
23. ↑ Vesatec (13-02-98)
24. ↑ Angeloso, en conversación privada
25. ↑ Sentenciado el caso del «Jamón y el vino». Wicho. Microsiervos (24-06-05)
26. ↑ Primera condena en España por distribuir ‘cracks’ en una página de Internet. El País (30/06/2005)
27. ↑ La policía cierra la “página del Jamón y el Vino”. Ángel Cortés. Noticias Intercom (28-05-97)
28. ↑ Sentenciado el caso del «Jamón y el vino». Wicho. Microsiervos (24-06-05)
29. ↑ PÁGINA CERRADA TEMPORALMENTE. Internet Archive (02-12-98)
30. ↑ es.comp.hackers. Google Groups
31. ↑ es.comp.hackers. News&Chats
32. ↑ historia*. A.H.E. - HackIndex (es.comp.hackers) (12/08/08)*
33. ↑ Nuestra historia*. A.H.E. - HackIndex (es.comp.hackers) (12/08/08)*
34. ↑ El Proyecto. Hackindex, Un Proyecto de Dominio Público del Grupo de Noticias es.comp.hackers (2001)
35. ↑ Nuestra historia. Hackindex (16-06-01)
36. ↑ Lista HackIndex
37. ↑ Información General. Lista de correo Hackindex. Elistas.net
38. ↑ CrackIndex
39. ↑ Nuestra historia. Hackindex (16/06/01)
40. ↑ IRC Vulcano
41. ↑ Operación SambaBios. Hackindex. Copia en Archive.org (13-12-01)
42. ↑ Operación SambaBios. Hackindex. Copia en Archive.org (13-12-01)
43. ↑ El grupo. Hackindex (07-12-03)
44. ↑ hacking*. News&Chats. “El País”, 1999*
45. ↑ Toni Panadès, en conversación privada
46. ↑ Documento fundacional de IRC-Hispano, colección privada de Toni Panadès
47. ↑ Resultados de la Encuesta: perfil del chateador. (31-10-99)

48. ↑ Secta #barcelona. Tranx Homepage (29-04-99)
49. ↑ Arrakis da el portazo al IRC HISPANO. Pedro de Alzaga. Diario del Navegante “El Mundo” (02-01-99)
50. ↑ Diccionario del IRC
51. ↑ Scytale: Channel Service. IRC-Hispano (18-01-98)
52. ↑ Mas cosas sobre Scytale (FAQ). IRC-Hispano (18-01-98)
53. ↑ Historia del IRC-Hispano. Sobre IRC-Hispano (18-08-01). Web Archive
54. ↑ Jesús Cea, comunicación privada
55. ↑ Juan Ignacio Rodríguez Tejada, en conversación privada
56. ↑ Jordi Murgó, en conversación privada
57. ↑ Juan Ignacio Rodríguez Tejada, en conversación privada
58. ↑ El zoo de Goku. Secta #barcelona. Tranx homepage (29-04-99)
59. ↑ Quien son y a que se dedican los IRCop y Cservice?, como se puede contactar con ellos?. FAQ de Ayuda Scripts por Lehenda
60. ↑ Historia del IRC-Hispano. Sobre IRC-Hispano (18-08-01). Web Archive
61. ↑ Comunicado de Arrakis publicado en www.irc-hispano.net/nueva_red.html. Diario del Navegante “El Mundo” (02-01-99)
62. ↑ Arrakis da el portazo al IRC HISPANO. Pedro de Alzaga. Diario del Navegante “El Mundo” (02-01-99)
63. ↑ Jordi Murgó, en conversación privada
64. ↑ Arrakis da el portazo al IRC HISPANO. Pedro de Alzaga. Diario del Navegante “El Mundo” (02-01-99)
65. ↑ Comunicado de Arrakis publicado en www.irc-hispano.net/nueva_red.html. Diario del Navegante “El Mundo” (02-01-99)
66. ↑ ¿Qué ocurrió con el #Alicante del Irc-Hispano.org?. Página web oficial del #ALICANTE
67. ↑ British Telecom compra uno de los mayores proveedores de Internet españoles. Pedro de Alzaga. Diario del Navegante “El Mundo” (13-01-99)
68. ↑ Ignasi Cavero, en conversación privada
69. ↑ Jordi Murgó. Twitter (05-07-13)
70. ↑ Toni Panadès, en conversación privada
71. ↑ ¿Quienes Somos?. Sobre IRC-Hispano (18-08-01). Web Archive
72. ↑ Sisco Sapena, reelegido presidente de iRC Hispano. Noticias.com (17-05-02)
73. ↑ IRC-HISPANO ELIGE NUEVO PRESIDENTE Y PRESENTA UNA NUEVA IMAGEN Y NUEVOS SERVICIOS. Notas Online (28-02-08)
74. ↑ Sisco Sapena, en conversación privada
75. ↑ Marco Castro. EX-IRC HISPANO (08-07-13)
76. ↑ Historia del IRC-Hispano. Sobre IRC-Hispano (18-08-01). Web Archive
77. ↑ Los fumetas resisten. Mercè Molist para “Ciberpaís” (05-99)
78. ↑ LA HISPANO.ORG HA DESREGISTRADO EL CANAL #CANNABIS POR TEMATICA ILEGAL. Hashito’s Peich
79. ↑ La Guardia Civil detiene a 17 personas e imputa a otras 13 por pornografía infantil en Internet. “El País” (10-03-2001)
80. ↑ Desarticulada una red de pornografía infantil que operaba en ocho provincias. *“El País” (23-03-2002)*
81. ↑ Desarticulada una red de defraudadores que insertaba publicidad pornográfica en canales de chat. Nota de prensa Guardia Civil (30-08-02)
82. ↑ IRC-Hispano: VISA sí. Mercè Molist para “Ciberpaís” (09-01-02)
83. ↑ El IRC-Hispano crece exponencialmente en agosto. Mercè Molist para “Ciberpaís” (08-99)
84. ↑ El IRC-Hispano crece exponencialmente en agosto. Mercè Molist para “Ciberpaís” (08-99)
85. ↑ La estadounidense PSINet compra Encomix y Abaforum. Juan Gonzalo. Diario del Navegante “El Mundo” (26-07-99)
86. ↑ ¿Quiénes Somos?. Sobre IRC Hispano (11-07-00)

87. ↑ Aquellos maravillosos scripts para mIRC. Jimmy. Pixfans.com (15-07-13)
88. ↑ Aquellos maravillosos scripts para mIRC. Jimmy. Pixfans.com (15-07-13)
89. ↑ http://web.archive.org/web/20130623191959/http://usuarios.iponet.es/dardo/amiga/tactic.htm *Tácticas de guerra en el IRC v.0.99a+]*. RoMaN SoFt/ LLFB (30/07/97)
90. ↑ Tácticas de guerra en el IRC v.4.1. RoMaN SoFt/ LLFB (20/09/99)
91. ↑ RoMaNSoFt, en conversación privada (02/02/09)
92. ↑ Santi Garrido: "No volvería a hacerlo". *Mercè Molist. Ciberpaís "El País" (16-02-06)*
93. ↑ *TaNiS*, en conversación privada
94. ↑ Colección privada de TaNiS
95. ↑ Comentario de BillSucks. Grupo EX-IRC HISPANO en Facebook (12-06-13)
96. ↑ *TaNiS*, en conversación privada
97. ↑ Windows NT/95/3.11 Out Of Band (OOB) data barf. Insecure.org
98. ↑ WinNuke
99. ↑ Wakanda (13-02-98)
100. ↑ Marco Castro en el grupo EX- IRC HISPANO de Facebook. (06-06-13)
101. ↑ Altair Div en el grupo Hackstory de Facebook (18-04-13)
102. ↑ Carles Mateu, en http://www.facebook.com/groups/hackstory/ (13-06-12)
103. ↑ lA nOchE. eL Qva$aR (10-03-99)

7. Enlaces externos

· Fidonet, aquellos maravillosos años. El blog de txipi (28-08-06).

7.1. Undercon

· UnderCon
· Undercon 97 a 2001

7.2. Isla Tortuga

· Isla Tortuga. Internet Archive.
· La Nueva Isla Tortuga
· Planeta Tortuga
· TOdO soBre el CaSo VESATEC / IsLaToRtuGa / Timofonica
· Web personal de Francisco Monteagudo
· Web personal de Ángel Badia
· Hackers. El underground español en Internet. IWorld (07/01/1998)
· COMUNICADO OFICIAL DE UNA DE LAS PARTES EN CONFLICTO EN EL CASO VESATEC. Angeloso (26/06/2005)
· Sentenciado el caso del «Jamón y el vino». Microsiervos (24/06/05)
· Boletín informativo de la Hwarez con motivo de los últimos acontecimientos relacionados con la página del Jamon y el vino. CyberIce'97.
· La tarifa plana sí es posible en España, explicada técnicamente por Francisco Monteagudo "Maki". Timofonicas.com.

7.3. es.comp.hackers

· es.comp.hackers
· FAQ de es.comp.hackers V 0.9.9 beta (13/09/01)
· FAQ de es.comp.hackers! Imprescindible!. Tutorial de Rojodos. Wikilearning.
· Hackindex. Copia de la web oficial en Archive.org.
· Lista de correu Hackindex. Elistas.net.
· Hackindex, la web de es.comp.hackers. Carlos Cortés. BULMA (12-11-01)

7.4. Lista de correo Hacking

· FAQ (preguntas y respuestas frecuentes) de la lista de correo hacking
· Suscripción a la lista
· Archivos de mensajes

7.5. IRC-Hispano

· History of IRC-Hispano. SearchIRC. IRC-Hispano.
· Comida de negocios con el IRC-Hispano. Marcos García Online (30-04-08)
· #Ayuda_IRC

· REGLAS EN CANAL #HACK DE IRC ESPAÑOL. Privateer. Underhack.
· Sisco Sapena: 'Si nadie paga no se podrá mantener ni lo gratuito'. *Mercè Molist. "Ciberpaís" (23-05-02)*
· Condenan a un pirata informático a dos años de cárcel y a pagar 1,4 millones de euros. "El País" (07-02-06)
· Logs divertidos del #barcelona. ag0ny's homepage (04-06-04)
· Script oficial de la SectaIRC. ag0ny's homepage (03-05-01).

7.6. La Vieja Guardia

· Web de La Vieja Guardia. Internet Archive.
· .:: RoMaNSoFt's ReSe@rch Labs ::.
· UnderSec Security Team

CAPÍTULO SEIS

Paranoia.com

Paranoia.com

“Este mundo es nuestro… el mundo de los electrones y los interruptores, la belleza del baudio. Utilizamos un servicio ya existente, sin pagar por eso que podría haber sido más barato si no fuese por esos especuladores. Y nos llamáis delincuentes. Exploramos… y nos llamáis delincuentes. Buscamos ampliar nuestros conocimientos… y nos llamáis delincuentes. No diferenciamos el color de la piel, ni la nacionalidad, ni la religión… y vosotros nos llamáis delincuentes. Construís bombas atómicas, hacéis la guerra, asesináis, estafáis al país y nos mentís tratando de hacernos creer que sois buenos, y aún nos tratáis de delincuentes.”

“Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y éste es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos… después de todo, somos todos iguales.”

The Mentor. Manifiesto del hacker *(08-01-1986)*

Estamos en 1995. Aparece en los medios de comunicación españoles la primera noticia -que se sepa- sobre la inseguridad informática del estado. Sorpresivamente, la noticia deja en buen lugar a los hackers. Llámalo la excepción que confirma la regla o la suerte del novato, nunca más volverá a darse tan extraña conjunción galáctica.

El 13 de octubre de 1995, prensa, radio y televisión destacaban una curiosa historia: tres estudiantes de Telecomunicaciones habían descubierto un agujero en el servidor web de La Moncloa y ellos mismos lo repararon. Esos angelitos eran **Álvaro Martínez Echevarría**, de 23 años, quien había descubierto el agujero, y sus compañeros **Roberto Lumbreras** y **Juan Céspedes**. Los chavales avisaron a la Moncloa del fallo y se ofrecieron a repararlo. Sorpresivamente -otra vez- el responsable de informática de la Moncloa, Juan Manuel García Varilla, no se enfadó con ellos ni les denunció por andar hurgando en su red. Todo lo contrario: aceptó su propuesta.

No queda claro, leyendo la prensa de la época, si fue Moncloa o los muchachos quienes fueron con el cuento a los medios. En todo caso, la noticia corrió como la pólvora. Los medios, que por aquel entonces sabían más bien poco de redes o informática, no se rompieron mucho la cabeza ante la versión que se les dio, ni se preguntaron qué estaban haciendo aquellos chicos cuando descubrieron el agujero. Para “El País”, por ejemplo, estaban realizando algo tan ¿normal? para un estudiante como un *“barrido rutinario de Internet”*:

> El pasado agosto, mientras llevaba a cabo un barrido rutinario de Internet, descubrió que la ventana Moncloa tenía un serio fallo de seguridad. Esta ventana lanza a Internet información general sobre las actividades de Presidencia del Gobierno.**[1]**



ABC

MADRID, LUNES 30 DE SEPTIEMBRE DE 1996

ASÍ PUDO ENTRAR ABC EN EL ORDENADOR DE LA MONCLOA

ABC publicó ayer los sorprendentes resultados de una investigación propia sobre seguridad informática en España y denunció la facilidad con la que cualquier persona con conocimientos técnicos puede penetrar en los principales ordenadores de nuestro país, entre ellos el del palacio de la Moncloa (en la imagen), y manipular o extraer datos, con consecuencias de incalculable gravedad. Durante la investigación, el equipo de redactores de ABC tuvo acceso a los ordenadores del «BOE», del CSIC y de la UNED. En la segunda parte del reportaje, que publicamos hoy, explicamos cómo fue posible burlar unos sistemas de seguridad que, en algunos casos, se podrían calificar de muy endebles. (Editorial en la sección de Opinión)

Josep Piqué

EL ESTADO INGRESARÁ MÁS DE MEDIO BILLÓN DE PESETAS POR LAS PRIVATIZACIONES DE REPSOL Y TELEFÓNICA

(«ABC, Diario de Economía»)

LOS PAPELES DE «POTOTO»: EMPRESARIOS Y BANQUEROS, EN EL PUNTO DE MIRA DE ETA

(Sección Nacional)

F. Álvarez-Cascos

CASCOS: «EL GAL NO ES TERRORISMO DE ESTADO, SINO TERRORISMO DE BODEGUILLA RELACIONADO CON PERSONAS DEL ENTORNO DE GONZÁLEZ»

(Páginas interiores)

Portada del diario "ABC" (30-09-96)

Un año después, en septiembre de 1996, el diario "ABC" publica otra bomba informativa. Cabe decir que la seguridad informática y los hackers eran algo tan raro en los 90, para la gente media y para los medios, como que un hombre muerda a un perro, y así lo trataban, como una curiosidad que llamaba la atención y por eso merecía amplia cobertura. Por eso es destacable la noticia de "ABC": porque parecía tomárselo en serio.

Este veterano periódico publica en 1996 un amplio reportaje que ofrece a portada y en dos entregas. Lo titula *"ABC demuestra la inseguridad informática de los principales organismos del estado"*. El texto explica que dos hackers anónimos han mostrado a los redactores del diario cómo de fácil es entrar en ordenadores del Centro Superior de Investigaciones Científicas (CSIC), la Universidad Nacional de Educación a Distancia (UNED), el Boletín Oficial del Estado (BOE) y La Moncloa.

Los hackers han usado un viejo truco: un programa del sistema operativo Unix, llamado PHF[2], tenía un agujero que muchos administradores no habían *parcheado*. Si alguien aprovechaba este fallo, podía descargar cualquier fichero del ordenador atacado, incluida la lista de usuarios y contraseñas. Sólo con que hubiese una contraseña débil -y había muchas, incluso usuarios sin contraseña- el hacker estaba dentro.

Según “ABC”, después de la demostración las contraseñas se pusieron a disposición de un notario y los hackers no hicieron nada malo en los sitios atacados, excepto demostrar que podían atacarlos. Pero, según el diario, se podían haber realizado un montón de inquietantes hazañas: robar información, sacarse un título en la UNED, cambiar leyes en el BOE, cambiar la agenda del presidente del gobierno...

El reportaje acaba con una frase lapidaria:

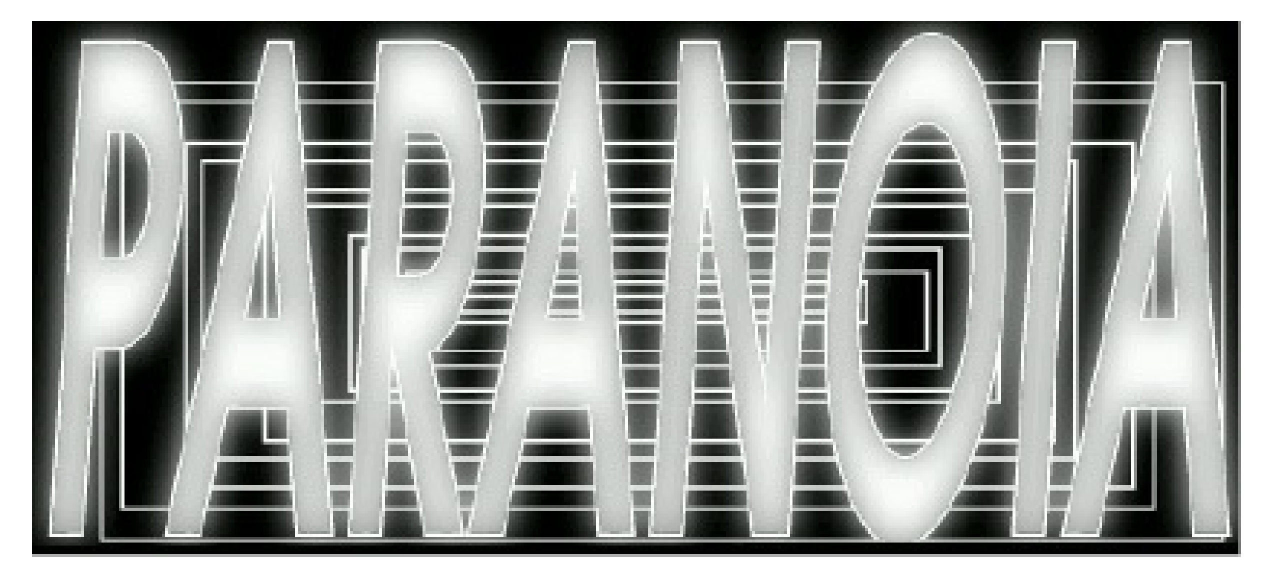
> Hoy por hoy, la seguridad informática en España es poco más que una quimera.[3]

Tienen razón. A mediados de los 90, en la mayoría de ordenadores conectados a las redes no hay barreras que paren los pies a los curiosos. Ni cortafuegos, ni contraseñas fuertes. Hay servidores en las universidades que llevan años en marcha sin que nadie los administre. Las redes han crecido en un ambiente de confianza y de buena fe. No es que los administradores de sistemas sean negligentes: es que no forma parte de su cultura securizar la red.

De hecho, instalar medidas de seguridad está mal visto por la élite de las universidades, la primera generación, que las ve como un constreñimiento, un engorro y un freno a la libertad de la información. No tienen en cuenta que crecen exponencialmente las hordas de jóvenes que van a robar y mentir por tener acceso vitalicio y gratuito a Internet. A toda Internet. Incluidos ordenadores “interesantes” como los de grandes empresas, universidades y militares.

Y así, nunca hacer hacking fue tan fácil, con todo abierto. Internet se convierte en una ciudad sin ley donde campan a sus anchas personajes de todas las calañas que entran y salen de donde les da la gana. Por no hablar de los contenidos que ofrecen algunos de los primeros sitios web: informaciones inmorales, ilegales y políticamente incorrectas. Desde toneladas de páginas pornográficas hasta warez, todo un mundo bizarro, como puede verse en el veterano sitio Paranoia.com, en pie desde junio de 1994 en la World Wide Web.

Paranoia.com afirma alojar a amigos y conocidos “a cambio de la voluntad”, en su interior hay webs de pedofilia, drogas, prostitución, eutanasia, cracking de televisión, teorías conspirativas y control mental. Lo fuerte es que Paranoia.com no es la excepción sino una más de las muchas páginas y foros de este estilo, fácilmente accesibles a cualquiera que entre en Internet.



Una gran sensación de impunidad flota en el ambiente. Para los que cuelgan contenidos políticamente incorrectos y para los que entran y salen de ordenadores ajenos. Este es un nuevo mundo y hacemos lo que nos da la gana, parece ser el lema. Las fuerzas de la ley no tienen conocimientos de redes ni informática. En aquellos primeros años, las investigaciones las realizan los propios atacados o los llamados *Computer Emergency Response Team* (CERT), "Equipos de Respuesta a emergencias informáticas". El primero en España es el esCERT, creado en la Universitat Politècnica de Catalunya en 1995, bajo el liderazgo de Manuel Medina. Le sigue, casi al mismo tiempo, el IRIS-CERT, cuyo territorio son las redes de las universidades españolas y lo dirige Rubén Martínez.

Los CERT son la respuesta de la comunidad de Internet a la necesidad de más seguridad informática. Empiezan ubicándose en universidades, siendo el primero el CERT de Carnegie Mellon. Su misión es ser un punto central de ayuda y coordinación ante ataques informáticos. La comunidad ha descubierto que necesita estos organismos a raíz de un incidente que pasará a la historia de Internet: el *gusano de Morris*:

> El 2 de noviembre de 1988, un programa dañino empezó a comerse ordenadores del sistema Arpanet. Saltó de uno a otro, de Arpanet a Milnet, a la NASA, al Massachusetts Institute of Technology, a las universidades, aprovechando varios errores en programas UNIX. Miles de máquinas colapsadas y el pánico general fueron el resultado de este gusano (virus que se "cuela" sin ayuda, con la única función de utilizar espacio del disco hasta estropear el sistema). Lo llamaron "gusano de Morris" por su creador, Robert Morris Jr, hijo de un científico jefe del National Computer Security Center.**[4]**

El Mundo Real elaboró también su respuesta a la inseguridad en la red: en 1995 se crea el Grupo de Delitos Informáticos del Cuerpo Nacional de Policía, dirigido por el veterano inspector jefe Carlos García**[5]**. Un año después se ponía en marcha el Grupo de Delincuencia Informática de la Guardia Civil, bajo el mando del teniente Anselmo del Moral, quien por sus declaraciones provocadoras a la prensa**[6]** y múltiples detenciones que realizó, con discutibles *modus operandi* que no siempre aceptaron los jueces, fue el policía más odiado de la red en los 90.

El primer detenido por hacking en España es Mave, del grupo Konspiradores Hacker Klub, en 1995 y quien lo detiene es Carlos García, de la Policía Nacional. A esta la

seguirán otras operaciones de ambos cuerpos que obligarán a los hackers ibéricos a esconderse y subir el nivel de paranoia. Por suerte para ellos, hasta el 2010 el Código Penal no considerará delito el hacking. Muchos se salvarán por eso. De lo que no se salvarán es de ser tratados como terroristas cuando se les detiene y criminalizados tanto por las fuerzas de la ley como por los medios de comunicación.

Un caso ilustra muy bien esta criminalización: a D.O.C., un joven de 22 años, de Águilas (Murcia), la Guardia Civil le detuvo en 1999 por presuntamente haber intentado robar el fichero de contraseñas del servidor web del Ministerio del Interior. El trato que recibió fue desproporcionado: estuvo encerrado seis días, sin fianza, en el depósito del juzgado de Lorca mientras el diario "ABC" lo llamaba terrorista. Su padre contratacó hablando con "El País":

> A las 12 del mediodía, nueve agentes de la Guardia Civil, algunos desplazados desde Madrid, irrumpían en su casa "como si fuera una operación comando, tratándolo como a un terrorista", se queja su padre, Ramón Ortiz, respetable empresario de la pequeña ciudad, de 20.000 habitantes.
>
> "Nadie le va a quitar el trauma por las medidas irracionales y desproporcionadas que se han tomado contra él, retenido 5 días ya en una habitación de 5 metros cuadrados, sin ventana y con un agujero por váter, sólo porque su número de teléfono empieza por 9684 y en su habitación encontraron un libro llamado "Hackers"".**[7]**
>
> "Nos han hundido psicológica y socialmente. El chico tuvo que irse del pueblo para trabajar. Y, al final, resulta que no había pruebas, buscaban un cabeza de turco".**[8]**

Tres años después, un juez sobreseyó el caso.

1. Konspiradores Hacker Klub

Konspiradores Hacker Klub (KHK) fue uno de los primeros grupos de hackers españoles, activo al menos en 1994 y 1995, dedicado al phreaking, ingeniería social y hacking, como la mayoría de grupos de aquel entonces, que tocaban un poco de todo. KHK remitía al nombre de la sala donde se reunían, en el restaurante Wendy's de la Puerta del Sol de Madrid: *"El salón de los conspiradores"*. Se habían conocido en la BBS del Demonio, en los encuentros que montaban los usuarios de la misma. Eran 5, todos madrileños menos un gallego, **Lester**.

> Nos juntamos un pequeño subgrupo apasionado de la informática y las comunicaciones, y un ansia infinita por aprender. Más que un grupo hacker eramos un grupo de amigos, que en realidad nos movíamos bastante individualmente pero compartíamos conocimiento enseñándonos unos a otros. No eramos como los grupos más modernos... no había afan de protagonismo, ni dejar nuestra marca por todas partes, ni hacer daño en ningún sitio.... solo aprender y aprender...**[9]**

El grupo tiene el triste honor de contar entre sus filas con el primer detenido por hacking en España: **Mave**. El 31 de en enero de 1996, la Brigada de Delitos Informáticos de la Policía Nacional irrumpió en la casa del joven, que entonces tenía 19 años. La policía llevaba un tiempo monitorizando el chat donde se reunía KHK, en EFnet, y por las conversaciones habían descubierto en qué ciudad residían. Un día, Mave cometió un grave error: entró en el IRC con una cuenta que contenía su nombre real.

> En el sumario estaba señado en circulo rojo y en grande "BINGO!!!!!" donde en el log del irc decía que tenía mi mismo apellido... Empezaron a buscar por el padrón municipal a todos los de mi apellido... y a pincharles el teléfono unos días.. como no había modem, pues al siguiente... hasta que encontraron una línea con módem todas las noches.**[10]**

Los cargos contra Mave fueron *"interceptación de telecomunicaciones"* y *"falsedad de identidad"*. Cuando le dejaron libre, el joven mandó de inmediato un mensaje a KHK, donde avisaba del peligro y explicaba que le acusaban por pasearse como Pedro por su casa por las redes de la Universidad Carlos III:

> Me han hecho toda clase de preguntas. Las dos principales vertientes por las que me acusan son la de usar tarjetas de credito en compuserve, usando el buzon de otra persona para recibir las cartas. De esto ultimo, el usar un buzon de otra persona, viene la acusacion de falsa identidad. La otra vertiente es la de haber entrado sin permiso en los ordenadores de la Carlos III, en concreto citaron 'Elrond', 'Ordago', 'Lareal', y 'a01-unix'. De esta vertiente me acusan del delito de 'Interceptación de las comunicaciones'. En este delito han metido la entrada a maquinas de la carlos III, el que yo supuestamente he 'leido' el correo privado de algun usuario, asi como la colocacion de sniffers, mediante el cual podia conseguir 'logins y palabras de paso de otros usuarios' segun sus palabras.**[11]**

Era el primer caso de hacking con el que se enfrentaban las fuerzas de la ley españolas, que fueron especialmente meticulosa pues el sumario de la investigación ocupaba tres tomos, unas 2.000 páginas. Pero no fue la policía quien realizó el grueso de las pesquisas sino expertos del sitio atacado, como solía pasar aquellos primeros años. Según Mave, el 90% de la investigación la realizaron

técnicos de la Universidad Carlos III, quienes descubrieron las intrusiones del grupo y el chat donde se reunía, que monitorizaron. Las pruebas que se presentaron al juez consistieron básicamente en los logs de IRC y -eso sí fue cosa de la policía- grabaciones de las conversaciones telefónicas de Mave.

El juicio nunca se realizó: *"Mave se comió el marrón y no dio ningún nombre. Consiguió no ir a la cárcel por los pelos pero tuvo que pagar una multa importante"*[12], explica Lester y lo confirma Mave:

> Fueron casi dos años de espera para el juicio. Al final, lo único que tenían en firme eran algunas confesiones del interrogatorio inicial y accesos a Compuserve de la última época. Hubo un pre-acuerdo a la entrada del juicio, aceptando la pena mínima (sin prisión) y una buena indemnización para la universidad. Me consta que al policía jefe (ya jubilado por lo que sé) no le sentó bien lo del acuerdo...;-)[13]

1.1. Mensaje de Mave

Por su valor documental, reproducimos algunos fragmentos del mensaje que Mave mandó a sus amigos de KHK justo después de la detención:

> Hola, soy Mave
>
> Lo que os voy a contar ahora es DE VITAL IMPORTANCIA. VUESTRO FUTURO ESTA EN ****PELIGRO**** MUCHO ****PELIGRO****
>
> Esta mañana del dia 31 de Enero de 1996, a las 9 de la mañana se ha presentado en mi casa la policia judicial, concretamente de la brigada de delitos informaticos, y me han ** DETENIDO **
> (...)
>
> Bueno, he visto cantidad de pruebas ABRUMADORAS, *MILES* Y *MILES* DE MENSAJES DE IRC hablando con toda clase de gente de toda clase de temas, que se remontan por lo que he podido recordar sobre alguna de ellas a mas de 1 año y medio hacia atras en el tiempo, tal vez 2 años.
>
> Tambien tenian TODAS mis converaciones de voz grabadas desde hace alrededor de 1 año quiza algo menos. Conversaciones con toda clase de gente, con otros hackers (vosotros sabreis con todos los que he hablado por voz en el ultimo año), con gente del mundo warez, con amigos, con todo el mundo que he hablado. (...)
>
> Me han preguntado sobre si conocia las identidades de algunas de las personas que salen en los log (principalmente de irc). Simplemente he contestado que solo conozco los alias, que no conozco los nombre reales. (...)
>
> Al principio de la declaracion me han preguntado que donde encontre los telefonos de acceso a la carlos III, y donde consegui los logins y passwords de entrada a alguna maquina. Mi respuesta ha sido que los encontre en la 'red' segun figura en la declaracion, aunque yo dije que los encontre por ahi, que no recuerdo exactamente donde.
> (...)
>
> Tambien me preguntaron literalmente 'šQue es lo que hay en Finlandia?'. Aqui ya no se que pensar, si es que son subnormales o es que no tienen ni puta idea del tema. Jamas he tocado

ninguna maquina de finlandia, ni he hablado con absolutamente nadie de hackear en Finlandia. Como todo el mundo sabe, en finlandia lo unico que hay es el remailer anonimo de anon.penet.fi.
(...)

Por lo que he conseguido averiguar estan investigando a otras personas, no me han dicho ni nombres ni alias... creo imaginar quienes pueden ser, y estoy seguro que si estais leyendo esto sabreis quienes soys...

Un consejo, *DESTRUID* *ABSOLUTAMENTE* *TODO* tanto en forma datos como de papel que podais tener que os pueda inculpar en algo... Si teneis algun programa comercial, *DESTRUIDLO* (Sobreescribirlo con 0 o similar, no lo borreis, para que no se pueda recuperar)... Y no useis en *ABSOLUTO* en telefono de voz... usad cabinas, PUBLICAS (no las de dentro de las universidades y similares) llamando a numeros a los que tengais ABSOLUTA certeza de que no estan pinchados...
(...)

Durante cierto tiempo, hace bastante tiempo, estuve sospechando (y ahora me doy cuenta que tenia toda la razon y no era ninguna paranoia) que tenia la linea pinchada. Los sintomas que se detectaban, el mas gordo fue, una llamada de cierta persona que no habia forma de cortarla, colgase yo, o colgase la persona que originaba la llamada, la linea seguia abierta. Alcabo de una media hora o asi, la linea recupero su estado 'normal'. Otro sintoma, fue la existencia de FALSOS RINGS, es decir el telefono sonaba, descolgabas y te daba linea. Es igual que los RING BACKS. Otro sintoma bastante delatador, fue la aparicion de RUIDO en las llamadas por modem a los que nunca antes habia tenido NINGUN problema de ruido.

Todo esto estuvo ocurriendo durante un periodo aproximado de 1 mes. Despues desaparecieron todas estas extrañezas, y el telefono se comportaba de lo mas normal. Muchisimas veces, intente hacerle PERRERIAS a la linea para detectar posibiles pinchazos, es decir microcuelgues, cuelges muy rapidos de la linea, cortar una llamada de golpe y ver si volvia a dar linea o seguia abierta la comunicacion (...). En ningun momento de estos test pude detectar ninguna anomalia. Sin embargo, por las transcripciones de conversaciones de voz que he visto, estas se realizaron en la epoca que hacia esas comprobaciones.

Sobre la linea contar una cosa que si que me parecio MUY CURIOSA, y que ahora estoy seguro de que es la prueba definitiva para detectar la linea pinchada, al menos con el metodo que usaron conmigo. (...) Siempre habia leido que el voltaje de la linea es de 48 voltios cuando esta colgado, y de 9-12 voltios cuando esta descolgado. Pues bien, mi linea al descolgarla tenia 27 voltios, en vez de los entre 9 y 12 que deberia esperar. *COMPROBAD* *AHORA* *MISMO* *EL* *VOLTAJE* *DE* *VUESTRA* *LINEA*.

Despues de unas 3 o 4 horas de declaracion, me han dejado en libertad. (...)

Ah, otra cosa. AVISO A TODA LA GENTE DEL WAREZ. Saben quienes son, que hacen, como lo hacen, etc. Todos aquellos que venden warez, QUE TENGAN MUCHISIMO CUIDADO. Yo de ellos destruiria todo el WAREZ (*DESTRUIR*), por lo que pueda pasar...

Cualquier comunicacion que hagais sobre este tema, hacedla de forma electronica, no useis ningun canal de voz, y HACEDLO TODO **ENCRIPTADO** con PGP, usando versiones *************** ANTERIORES ************* a la 2.6ui. En principio la 2.6ui es segura. Lo de la version, es por la rumoreada backdoor de las versiones > 2.6 que obligo a instalar a zimmerman el fbi/cia para poder desencriptar facilmente los mensajes. Despues de cierto

comentario que ha hecho uno de los policias, estoy casi ABSOLUTAMENTE seguro de que esa backdoor existe y es TOTALMENTE CIERTA. (...)

Muchisimas Gracias, y tened MUCHO cuidado.
Mave.**[14]**

2. Universitat Rovira i Virgili

La segunda detención por hacking en el estado español la llevó a cabo el recién creado Grupo de Delitos Informáticos de la Guardia Civil y la provocó también hacer el indio en una universidad: la Universitat Rovira i Virgili (URV) de Tarragona. A finales de 1996 la URV puso una denuncia que llevó a la detención, en marzo de 1997, de **J.H.R.** y **J.D.M.**, de 20 y 19 años respectivamente. Ambos estudiaban primer curso en la Escuela Técnica Superior de Ingeniería de la URV.

Se les acusó de intrusión en redes informáticas para cometer delitos contra la propiedad intelectual y revelación de secretos. El rosario de sus presuntas andadas durante aquel curso 1996-97 comprendía ataques a ordenadores de las universidades de Valencia, Málaga y Córdoba, el Centre de Supercomputació de Catalunya, el congreso INETCAT'96, una empresa de Canarias, la red ciudadana de Tarragona TINET y el Registro Mercantil de Tarragona, además de vender CDs copiados ilegalmente.

Según la denuncia de la URV, habrían robado las contraseñas de más de 2.000 alumnos y entre 100 y 200 profesores y entrado en las cuentas de dos profesores[15]. En su lista de gamberradas destacaban borrar la información que de ellos tenía la biblioteca referente a libros en préstamo y suplantar la identidad de un ejecutivo para conseguir información de una empresa de seguridad informática.[16]

El fiscal pidió para J.H.R. tres años de cárcel y 378.000 pesetas. Para J.D.M., dos años y siete meses de prisión, más multa de 306.000 pesetas.

El Grupo de Delitos Informáticos de la Guardia Civil se estrenaba con esta investigación, que duró tres meses y a la que llamó *Operación Toco*[17], porque *Toco* era uno de los apodos que usaba J.H.R.[18], conocido también como *Tranx* en el IRC.

2.1. El sumario

El sumario de la investigación presentaba a J.H.R. como principal responsable de los delitos pero, según explicó a la prensa, su compañero lo traicionó para que pareciese el único culpable:

> Según H., su compañero le acusó de ser el cabecilla y único responsable de las intrusiones. En un día pasaron de ser íntimos amigos a amables enemigos.[19]

En cuanto a los delitos de hacking que presuntamente habían cometido los acusados, el sumario explicaba que J.H.R. usó un código de usuario de J.D.M. para entrar en la red de la URV y poner un programa llamado sniffer en un ordenador de la universidad, que grabó toda la información que se introducía en él. Así fue como consiguió la contraseña del administrador que controlaba todo el sistema informático de la universidad.

Desde la cuenta de administrador fue fácil obtener el fichero ALUMNE.TXT, con las

contraseñas de más de 2.000 alumnos, además de los códigos de usuario y contraseñas de entre 100 y 200 profesores. Los jóvenes aprovecharon esta información para chiquilladas como espiar el contenido de exámenes, pero también para entrar en ordenadores de las universidades de Valencia, Málaga y Córdoba, ya que muchos usaban la misma contraseña en diferentes cuentas. Desde allí saltaron a sitios más "interesantes", como el Centre de Supercomputació de Catalunya o el Registro de la Propiedad de Tarragona, donde según el sumario entraron en diversas ocasiones para coger informaciones sin pagar.

Fue especialmente sonada su visita física al congreso INETCAT'96, celebrado entre el 27 de noviembre y el 1 de diciembre de 1996, que organizaba la Internet Society catalana y de donde fueron expulsados[20]. Según el sumario, habrían atacado un ordenador del congreso:

> J.H.R. en compañía de otras personas se hallaba en el stand de la empresa I3D, (...) a través de un ordenador de Pangea accedió a un ordenador de la Rovira i Virgili y desde allí lanzaron un ataque al ordenador del congreso ROSETTA INETCAT PANGEA ORG. Introduciendo un elevado número de conexiones para que el ordenador del Congreso se bloqueara.[21]

Pero en los registros que la Guardia Civil hizo a los domicilios de los jóvenes no encontró ninguna prueba.

2.2. El juicio

El juicio contra J.H.R. y J.D.M. se celebró en mayo de 2005, en el Juzgado de lo Penal número 4 de Tarragona, rodeado de gran cantidad de cámaras y periodistas. Habían pasado nueve años desde las detenciones y el principal denunciante, la Universitat Rovira i Virgili, se había echado atrás. Fuentes de la universidad afirmaron a la prensa, en 1999, que no esperaban que el caso llegase a juicio cuando pusieron la denuncia:

> La primera intención de la universidad no iba más allá de que los jóvenes recibieran un pequeño rapapolvo académico.[22]

La única parte acusadora en el juicio fue el ministerio fiscal. Un representante de la universidad, Manuel Sanromà, que habló como parte afectada, criticó la actuación de las fuerzas de la ley:

> Aseguró ante la juez que los hechos habían sido sólo "una gamberrada": presuntamente, pintar cuernos a las fotografías de profesores, espiar exámenenes, copiar contraseñas o buscar información sobre libros en la biblioteca de la Universidad de Valencia. Sanromá calificó la actuación judicial de "desproporcionada".[23]

Sanromà no fue el único que criticó al Grupo de Delitos Informáticos de la Guardia Civil, que no asistió al juicio. Uno de los acusados, J.D.M., denunció que le habían prometido trabajo a cambio de su colaboración:

> J.D.M. aseguró haber hecho sus primeras declaraciones presionado por la Unidad de Delitos Informáticos de la Guardia Civil: "Nos habían vigilado, pinchado el teléfono y venían expresamente de Madrid. ¡Imagínese! Sugirieron que si colaboraba podría trabajar con ellos y que ya me llamarían". Jaime Duque, uno de los abogados defensores, se quejó asimismo de

> esta unidad de la Guardia Civil que "bajó desde Madrid para montar una bomba de humo. Se hicieron la foto de rigor con ordenadores y disquetes en los que no había nada y ninguno de ellos está hoy aquí para explicar cómo fue la investigación previa".[24]

La inexperiencia de los agentes quedó patente en la debilidad de las pruebas y las imprecisiones del sumario, que fueron criticadas por todas las partes, también los péritos de la acusación. Destacó además en este juicio la ignorancia del juez y el fiscal en todo lo relativo a seguridad informática. Finalmente y ante la inconsistencia de las pruebas, el juez absolvió a los jóvenes.

2.3. Descontrol en las universidades

Cuando J.H.R. y J.D.M. fueron detenidos, en 1997, las universidades eran el gran campo de juego de la comunidad hacker, especialmente los más jóvenes, alumnos de estas instituciones. El sumario del caso destacaba que, aunque J.H.R. era alumno de la URV, no asistía nunca a clase[25], pero lo que se presentaba como una anomalía era en realidad algo habitual: en vez de ir a clase, campaban a sus anchas por las aulas de ordenadores y las redes de las universidades, entrando y saliendo de todas partes, usando las máquinas asaltadas para montar chats, almacenar warez o saltar a otros sitios. Muchos jamás acabaron la carrera, pero se licenciaron de forma autodidacta en una asignatura entonces inexistente: seguridad informática.

Las universidades, con poco personal, poco formado e interesado en seguridad, muchos ordenadores y muchos usuarios eran el gran agujero de Internet. No había incidente de hacking en los 90, protagonizado por alumnos o por gente más avezada, que no implicase el asalto previo a algún sistema universitario. De allí se saltaba a otro y a otro, hasta llegar al objetivo, complicando así el rastreo policial.

El Equipo de Respuesta a Incidentes de RedIRIS (IRIS-CERT) tenía la ingrata misión de velar por la seguridad de las redes universitarias y de investigación españolas. En 1999 genera sus primeras estadísticas públicas, donde afirma que ha atendido 240 incidentes durante aquel año. De ellos, 38 son accesos ilegales o ataques de denegación de servicio (bombardeos), y hay también 30 intentos de entrada en sistemas.

Hay que decir que estas estadísticas reflejaban sólo los ataques denunciados al IRIS-CERT. En realidad había muchísimos que ni siquiera se detectaban. Y la mitad de los que se denunciaron no se solucionaron jamás.[26]

Año a año, los incidentes registrados por IRIS-CERT se iban doblando: 490 en el 2000[27]. 1.065 en 2001. 1.495 en 2002....[28]

Si los atacantes eran alumnos, la pillería más común era robar contraseñas de profesores, porque ellos tenían acceso completo a Internet, mientras los alumnos sólo tenían correo electrónico. Miquel Barceló recuerda como sus alumnos de la Universitat Politècnica de Catalunya (UPC) le robaron la contraseña de acceso a servicios privilegiados mediante la manida técnica del espiar a alguien por detrás

mientra está tecleando.

En este contexto de cada vez más descontrol y desvergüenza puede entenderse que algunas universidades concluyeran que avisar a la policía sería un buen escarmiento. Es en esta clave como debe leerse la actuación contra J.H.R. y J.D.M. en la Rovira i Virgili o, por parte de la Politècnica de Catalunya, la denuncia que llevó al caso !Hispahack.

3. El Caso Hispahack

El llamado **Caso** Hispahack se refiere a la investigación, detención y posterior juicio contra este grupo de hackers. !H no fue el primero ni el segundo en ser pillado por las fuerzas de la ley, pero sí el que tuvo más publicidad.

La investigación, llevada a cabo por el Grupo de Delitos Informáticos de la Guardia Civil, empezó en 1997 y culminó en abril de 1998, con cuatro personas detenidas, acusadas de entrar en sistemas de universidades, proveedores de acceso, el Congreso de los Diputados, la NASA y una larga ristra. Finalmente, la presión judicial se concretó en *Jfs*. El fiscal pedía para él dos años de prisión por, presuntamente, entrar en una máquina de la Universitat Politècnica de Catalunya (UPC) y transferir datos de allí a un ordenador de Palma de Mallorca. Nombre de usuario: !HISPAHACK. Directorio: Jfs. Parecía tenerlo todo en contra pero, al final, en mayo de 1999, el juez le absolvió por inconsistencia de las pruebas.

El *Caso Hispahack* es el más importante de la historia del hacking en España por diversas razones. Para empezar, fue la primera redada dirigida específicamente contra un grupo hacker, acusado de delitos de hacking. Hasta entonces, las detenciones se habían centrado en individuos concretos y aunque formasen parte de un grupo, no se había dado importancia a este hecho. Ahora en cambio, la Guardia Civil en su nota de prensa daba más relevancia al grupo que a los detenidos, calificando a !Hispahack de banda organizada:

> Del Moral cuenta que los intrusos han mostrado en todo momento una actitud "fría e inteligente". Según sus datos, Hispahack es la red de delincuencia informática más importante desbaratada hasta ahora en España. El Grupo de la Guardia Civil trabaja en colaboración con el FBI y con la policía británica para aclarar las incursiones realizadas en ordenadores de sus países.**[29]**

El Caso Hispahack es también la muestra de cómo un grupo de hackers respetable y respetado puede acabar pasando a la historia como un grupo de circo y cómo su pericia puede verse eclipsada por noticias peliculeras de asaltos a la NASA o el Pentágono. Sensacionalismo surgido de una Guardia Civil ávida de salir en los medios, y de unos medios totalmente ignorantes, ávidos de temas sobre *malvados hackers*.

A nivel legal, en cambio, la aportación del Caso Hispahack es muy seria y valiosa, pues dio lugar a la primera sentencia en el estado español sobre acceso ilegal a un sistema informático. Aunque J.H.R. y J.D.M. habían sido detenidos antes, en marzo de 1997, también por la Guardia Civil, no se les juzgó hasta 2005. Así que el Caso Hispahack fue el primer caso de hacking que llegaba a un tribunal y fue seguido muy de cerca por toda la abogacía interesada en estos temas. Aunque dio lugar a una sentencia discreta, no defraudó, sentando diversos precedentes que hasta entonces levantaban dudas, como la aceptación de los logs generados por sistemas informáticos como prueba en un juicio.

3.1. Qué fue lo que pasó

Presuntamente, había algunos chavales en !Hispahack que estaban disfrutando de lo lindo haciendo el indio por las redes informáticas, junto a amigos como el propio J.H.R.

Para hacerse una idea de lo bien que lo pasaban es interesante leer el informe que hizo el périto del esCERT, sobre lo que encontró en los dos ordenadores de Jfs requisados por la Guardia Civil:

> Hay ficheros de contraseñas presuntamente robados en máquinas de todo el mundo, desde Tailandia a Kiev pasando por Suecia, Canadá, Australia, universidades de Nevada, Yale y España e, incluso, un fichero moncloa.pwd y otro mil.pwd. En total, 9.459 cuentas, la mayoría aún no descifradas. Uno de los ordenadores tenía las salidas de dos “sniffers”, instalados en máquinas de las universidades de Barcelona y Oxford, en las que se habían introducido también puertas traseras de acceso como “root” (administrador). Existen evidencias de que Jfs tenía acceso libre a otros ordenadores de Gran Bretaña, Alemania y el CERN (Laboratorio Europeo de Partículas Físicas), en Suiza.**[30]**

Otro detalle que ilustra la gran actividad desplegada por aquellos hackers es una anécdota que suele contar el apòstol Jordi Murgó: un día, revisando los sistemas de la Universitat de Lleida por trabajo, se topó con Stk y Jfs**[31]**, que habían conseguido entrar y tomar el control de buen número de máquinas. Las usaban para sus cosas, como hacer funcionar en una de ellas el robot que llevaba las tareas de mantenimiento de su canal privado *#!hispahack* en Undernet. El veterano Murgó descubrió cómo entrar en el canal, les avisó de que les había pillado, cerró los agujeros, borró los programas troyanos y se lo tomó a broma.

Pero otros no estaban para bromas. Entre marzo y septiembre de 1997, Stk y un chaval ajeno a !H, Magne, presuntamente robaron la base de datos de usuarios y contraseñas de un pequeño proveedor de Girona y los repartieron en el IRC. El proveedor, lleno de furia, empezó a investigar por su cuenta. Mientras, los alegres chicos de !H siguieron con sus aventuras. En su sensación de total impunidad olvidaron la bendita paranoia, patrona de los hackers, y Jfs y _JR_ se dejaron hacer una foto en una *kedada*

Paralela y presuntamente, Jfs se paseaba por las redes de la Universitat Politècnica de Catalunya (UPC), a pesar de ser lo boca del lobo más negro, pues allí residía el primer equipo de investigación en ciberseguridad que hubo en España, el esCERT. Según la denuncia de la UPC, Jfs asaltó 16 ordenadores y puso “sniffers” en 5 de ellos. Los *sniffers* son programas que graban todos los datos que pasan por un ordenador y se suelen usar para capturar nombres de usuario y contraseñas. Pero justo allí, en la boca del lobo, va Jfs y se equivoca al instalar uno de los “sniffers”, que acaba grabando sus propios pasos. A ese rastro se agarra el esCERT para seguirle la pista.

3.2. Jaque mate

El 20 de enero de 1998, el ISP de Girona pone una denuncia contra Magne y Stk,

este último presunto miembro de !Hispahack, ya que se conecta a la red con un dominio que lleva este nombre. El proveedor asegura que ambos chicos le han robado las claves de acceso y nombres de usuario de 2.500 clientes. Tres meses después, conminada por la Guardia Civil, la Universitat Politècnica de Catalunya pone también una denuncia, por el ataque, el 11 de septiembre de 1997, con la obtención de privilegios de administrador, contra 16 ordenadores de un departamento.

El ISP de Girona y el esCERT colaborarán con la Guardia Civil en la investigación, lo que en la práctica significa que el proveedor y el equipo de la UPC llevan a cabo el grueso del trabajo ya que, en aquella época, los conocimientos de seguridad informática de las fuerzas de la ley dejaban mucho que desear. La investigación revela que el asaltante de la UPC viene de un ordenador también asaltado de la Universidad de Oviedo. Después, ya en los ordenadores de la universidad catalana, ha programado los "sniffers" para que manden los datos capturados a un ordenador de un cibercafé de Mallorca.[32]

Para más inri, el nombre de usuario con que se entra al ordenador de Mallorca es "hispahack" y el directorio donde se guardan los datos lleva el nombre "jfs". Los peritos del esCERT descubren también que hay alguien más, con el nombre de usuario **thelobo**, que *"conoce la existencia y el contenido de la cuenta 'hispahack'"* pero no accede al ordenador a través de Internet sino físicamente, desde el cibercafé.

El 1 de abril de 1998, Jfs y Stk, de 21 y 22 años respectivamente, que trabajan en Gibraltar, reciben una invitación a visitar la comandancia más cercana de la Guardia Civil, en La Línea. Inocentes, incrédulos, van al matadero: nada más entrar, les encierran en un calabozo donde pasarán la noche. Stk se librará, pero para Jfs ha empezado un calvario. El mismo día, en Asturias, detienen a JR, de 26 años, un profesor de informática. A la mañana siguiente, cae Magne, en Barcelona. Hay además diversos imputados, como el abogado Carlos Sánchez Almeida, bajo el alias **Shooting**. Se les acusa de revelación de secretos y daños. Niegan todos los cargos excepto Stk quien, asustado, "canta" como un cosaco y, entre otras cosas, afirma haber hecho una conexión vía telnet a un ordenador de la NASA. La Guardia Civil se agarrará a esto para dar a los medios una imagen sensacionalista del caso.

3.3. Lo del Manda guebos!!

En declaraciones a "El País"[33], uno de los integrantes más respetados de !H, LeCrème, se mostraba convencido de que la persecución contra el grupo no se debió a estas travesura sino al deface de la web del Congreso de los Diputados de España, el 31 de octubre de 1997, donde alguien escribió:

Cuantos diputados y cuantas comisiones harán falta para descubrir que poner un ordenador en internet no es sólo enchufarlo [Manda guebos!!... 1-3, seguimos avanzando!] (!H)

Según “El Periódico”[34], la portada hackeada lució igual toda la semana, sin que nadie arreglase el desaguisado (la empresa TSAI, de Telefónica, era la responsable del servidor). Al final, un programa de radio sobre nuevas tecnologías en Onda Rambla, *Power-UP*, que dirigía Marc Bilbeny, avisó públicamente del *deface*.

A diferencia del mundo exterior, la hazaña corrió como pólvora en el “underground”, donde fue aplaudida. Apareció en las secciones de *Noticias* de diversas webs y ezines, como el de JJF Hackers Team:

> A principios de Noviembre el web del congreso español fue hackeada presuntamente por el grupo !H (no sera yo quien diga lo que significa :). Cuando conectas al web, aparecia una pantalla oscura con un grafico en el cual se veia un gran !H. Y debajo ponia la siguiente frase: “HAPPY HACKLOWEEN” y con otra que decia mas o menos “Señores del congreso, poner un web no es solo enchufar el ordenador.(!H)”[35]

Yandros, miembro de !H, aprovecha que ha pasado el tiempo para explicar que el ataque se fraguó en un canal de chat:

> Sobre la famosa web del congreso... esa noche había mas de una copa en el ambiente, y fue una chica la que lo hizo, valenciana sin ir más lejos :)[36]

Pocos días después del *deface*, el 2 de noviembre, alguien desde una dirección de correo anónima envía a la Guardia Civil la dirección de una página donde hay fotografías en las que aparecen miembros de !Hispahack, entre ellos Jfs y _JR_. Para hacer más fácil su identificación, los *nicks* están escritos encima de sus caras. No queda claro si esta página es la web oficial de !Hispahack en el alojador gratuito Angelfire o la Guardia Civil llegó a ella por otras vías. En todo caso, los agentes visitaron la web de !H y leyeron con mucha atención los artículos, nombres y direcciones de correo que allí aparecían.

DILIGENCIA DE INFORME.----------------------------------

---En Barcelona, siendo las 16:30 horas del 25 de Marzo de 1.998, el Instructor de las presentes hace constar el siguiente informe a SSª:---------------------------

---Con fecha de 2 de noviembre de 1.997 se recibió en la sede de este grupo de delincuencia informática en Madrid un mensaje de correo electrónico a través de Internet, en el cual se adjuntaba la dirección de Internet donde podian verse diversas fotografías de los miembros de un grupo de "hackers" o intrusos informáticos que se autodenominan HISPAHACK, los cuales al parecer habían accedido de forma ilegal al ordenador del Congreso de los Diputados en Madrid.-------------------------

---Puestos en contacto con el responsable técnico de dicho ordenador, éste confirmó los hechos, manifestando que, él o los atacantes habían modificado diversa información firmando los autores del acceso no autorizado como !HISPAHACK o !H . Dicha persona, tras ser informada de la posibilidad de denunciar los hechos, participó que estudiaría las posibles acciones legales y en caso de querer denunciar se pondría en contacto con esta Unidad, no habiéndose producido tal circunstancia hasta el día de la fecha.-------------------------------

Atestado del hack al Congreso de los Diputados, facilitado por el abogado Carlos Sánchez

Almeida.

La otra parte afectada por el *deface*, la compañía Telefónica de España, presentó al poco tiempo una queja -que no denuncia- a la Guardia Civil contra !Hispahack, por un intento de acceso a ordenadores de la NASA y de la Universidad de Oxford. De hecho, el ataque al Congreso se había realizado desde Estados Unidos:

> La NASA envió una queja a Telefónica porque alguien, desde España, había intentado asaltar sus ordenadores y había dejado la huella H!. Se verifica que el asalto venía de un proveedor de Girona, quien denuncia que le han sustraido las claves de acceso de 2.500 usuarios. **[37]**

Pero, como explicará el entonces comandante del Grupo de Delitos Informáticos de la Guardia Civil a la Comisión Especial sobre redes informáticas del Senado**[38]**, al no existir denuncias ni de Telefónica ni del Congreso de los Diputados, la investigación no podía ir más allá.

> Con respecto a estos tres casos, como pueden ustedes imaginarse, no pudimos hacer absolutamente nada porque no existía una denuncia oficial sino que simplemente se recibió información sobre ello.**[39]**

Por eso la Guardia Civil insistió a la UPC y el proveedor de Girona para que presentasen denuncia formal.

3.4. El juicio y la sentencia

Se pedían 2 años de prisión para Jfs y una indemnización a la UPC de 2.700.000 pesetas.

El juicio se llevó a cabo el 26 de mayo de 1999. La defensa, que llevaba el abogado Carlos Sánchez Almeida, se centró en que no había más prueba contra Jfs que el hecho de que su nick coincidía con el nombre del directorio del ordenador del cibercafé. Algo que el juez, Juan Carlos Llavona Calderón, consideró insuficiente para condenar al joven. Almeida convenció además a juez y fiscal, cuyos conocimientos de informática eran nulos, de que Jfs era un hacker blanco, que no hacía ningún daño.

> "¡Estamos ante un caso de "hacking blanco"!", acabó exclamando el propio fiscal, converso y emocionado, en el juicio de !Hispahack.**[40]**

Jfs fue absuelto**[41]** por considerarse los hechos denunciados probados, pero no atribuibles a su persona, ya que cualquiera, con el usuario "hispahack", podía entrar al directorio "jfs".**[42]**

Pero, a pesar de acabar en absolución, la sentencia gustó más a la Guardia Civil que a Carlos Sánchez Almeida, que la calificó de *"muy dura"***[43]** en aspectos como la intimidad de las personas, pues el juez no reprobó el hecho de que la policía, sin orden judicial, exigiese datos de usuarios a cuatro importantes ISPs y estos se los diesen; o que se investigasen cosas sin existir denuncia previa.

> Durante las pesquisas policiales, la Guardia Civil obtuvo información de diversos usuarios de Internet a través de las empresas proveedoras, en concreto Intercom, MrBit, Servicom y RedesTB. El caso extremo fue el de éste último proveedor, que llegó a facilitar a la Guardia

Civil, sin autorización judicial, el login y password de una persona cuyo único delito había sido firmar un artículo denunciando los abusos de Telefónica.[44]

También se criticó que el esCERT actuase como périto en el juicio, cuando era parte denunciante por su pertenencia a la UPC. Además, se aceptaron como pruebas los logs o registros de los movimientos que ha habido en un ordenador o sistema, algo discutido y discutible por el hecho de que, como ficheros informáticos, son fácilmente manipulables. Aunque, de hecho, a Jfs lo salvaron los logs, porque no aparecía en ellos.

Pero lo que más dolió a la comunidad fue que la sentencia criminalizase, por primera vez en el ámbito judicial español, la práctica del hacking, que definía como *"conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables y aún merecedoras de sanción penal"*[45][46].

Después de conocerse la sentencia, !Hispahack publicó en su web un documento, *En la hora de la victoria*, donde ofrecía una turbia versión sobre las causas de la actuación contra el grupo:

> La Guardia Civil actuó contra Mentes Inquietas porque en nuestro Web se publicó un artículo en el que se informaba de las extrañas amistades de fuerzas de seguridad con las multinacionales del software y las telecomunicaciones, y un artículo en el que se reproducían los derechos que asisten a todo detenido, recogidos en las leyes españolas.[47]

3.5. La exageración de los medios

La nota de prensa de la Guardia Civil donde se informaba de la redada contra !Hispahack tenía su toque de exageración, llamando por ejemplo al grupo "banda organizada". Pero los medios aumentaron exponencialmente este amarillismo gracias a su completa ignorancia y ganas de "carnaza". Destaca entre todos el artículo que dedicó al caso "El Periódico de Catalunya". Tendencioso sería el calificativo suave para aquel texto, donde las detenciones de unas personas presuntamente inocentes se mezclaron con otras historias cuya veracidad no se comprobó y que no tenían nada que ver con el caso, pero invitaban al lector a creer que sí.



2 TEMA DEL DÍA

Lunes, 1 de junio de 1998
Intrusos en la red
Tema del día

Vacío legal

Los 'ciberpiratas' españoles se cuelan en la NASA y el Pentágono

Un estudiante de la Politècnica entró en un satélite y movió sus placas solares

Otro 'hacker' manipuló el simulador de guerra atómica de Estados Unidos

Los saboteadores han espiado a importantes proveedores de Internet

NOTICIAS DE HACKERS

"El Periódico de Catalunya" dedicó dos páginas a la detención de !Hispahack

> EL PERIÓDICO ha localizado a un hacker catalán –dice estar retirado– que hace tres años se coló en la NASA y, con las contraseñas captadas, llegó al simulador de guerra atómica de EEUU. (...) Un estudiante de la Universitat Autònoma de Barcelona (UAB) logró entrar en la NASA con el intercambio de unas claves conseguidas en el Centre de Supercomputació de Catalunya. Llegó al sistema de control de misiones espaciales. Otro alumno de la Universitat Politècnica de Catalunya manipuló en 1995 el programa de control de un satélite sin saber dónde estaba. Sus manejos hicieron que se moviera uno de los paneles solares y que dejara de recibir energía del sol. Tiempo después se pudo arreglar el pequeño estropicio. El estudiante fue castigado.[48]

Para completar el artículo se añadía una entrevista a Maki y Angeloso, que nada tenían que ver con el caso, detenidos un año antes por temas de warez y carding a raíz de una denuncia de la Business Software Alliance contra Isla Tortuga.



Invasiones en ordenadores de América y Asia

LA TERMINOLOGÍA

Una jerga para la comunicación entre iniciados

Jamón, vino y Timofónica

'Webs' de protesta contra Telefónica llevan al juzgado a varios internautas

Segunda página del reportaje de "El Periódico de Catalunya" sobre el Caso Hispahack

En cuanto a los escasos medios que entonces operaban en la red, como "Noticias.com", del periodista Ángel Cortés, fueron más realistas e incluso denunciaron lo que consideraban un *"montaje policial"*. "Noticias.com" fue el único medio de comunicación donde aparecieron declaraciones de Jfs justo después de la detención:

> Lluís F.F., manifestaba "Estoy muy dolido, ni hemos entrado en la NASA ni nada, todo me parece una locura y una exageración de la Guardia Civil que hasta nos ha pinchado los teléfonos".**[49]**

3.6. La oscuridad

El principal efecto del Caso Hispahack en la comunidad hacker fue generar miedo, explica Almeida:

> Despertó un sentimiento de persecución, de Internet como zona peligrosa, y la consecuencia fue que los grupos se cerraron.**[50]**

El primer en cerrarse fue !H, que aunque siguió en pie nunca fue el mismo. Se hizo más "underground" y paranoico, el cifrado se convirtió en su fiel compañero, explica Yandros:

> Blindamos todas nuestras conexiones (en una maquina mía, por cierto), empezando a usar asiduamente protocolos de cifrado para todo lo que haciamos. Hasta ese momento, y por

> contra de lo que decia Anselmito del Moral, hablabamos en undernet sin ningun tipo de reparo :)[51]

La paranoia era y es clásica del mundo hacker, donde se traspasan límites con suma facilidad y está siempre presente el riesgo de que te pillen, pero ciertamente !H rizó el rizo, explica Zhodiac:

> Una caracteristica muy de !H fue lo cerrado (opaco, oscuro) que era todo. La gente en el underground espanyol no sabia quien era o dejaba de ser de !hispahack pk normalmente se publicaban con pseudonimos no reales. Eso era en la segunda etapa para la protección de los miembros ante nuevas embestidas policiales, y posiblemente infundadas. Eso era muy de !h, esa opacidad. Si alguien decia ser de !H muy posiblemente no lo era :)[52]

4. Operación Millenium

La Guardia Civil bautizó como Operación Millenium la detención de 55 personas en 16 provincias españolas, en enero del 2000, por presunto uso fraudulento de números de teléfono 900, los cuales correspondían a módems que permitían conectarse gratuitamente a Internet, pagando la factura la empresa propietaria de los mismos.

> La utilización de líneas 900 ajenas, cargando el coste a las empresas propietarias, es un hecho bien conocido y cuyo origen se remonta años atrás.**[53]**

Entre las empresas denunciantes destacaban Microsoft Ibérica, Toshiba y Novartis**[54]**. Según las mismas, el fraude alcanzaría la cifra de más de 50.000 pesetas por persona (menos de esta cantidad sería estafa, un delito menor) y las llamadas se habrían hecho desde 200 números de teléfono distintos.

La investigación, llevada a cabo por el Grupo de Delitos Telemáticos de la Guardia Civil, empezó en marzo de 1999, tras la detención en Madrid de una persona que hacía compras en Internet con tarjetas de crédito de terceros. Según los investigadores, esta persona pertenecía a un grupo de phreakers llamado **COM 30**, dedicado a diversos tipos de fraudes y delitos telefónicos, como divulgar en el "underground" números de tarjetas de crédito y de líneas 900. También clonaban tarjetas de móviles.**[55]**

Tras casi un año de investigación, la Guardia Civil localizó a los presuntos cabecillas de COM 30, **_X_** y **Danko**, residentes en Alicante y Córdoba respectivamente. Se les acusaba de proporcionar a otros internautas números de tarjetas de prepago pertenecientes a terceras personas, así como instrucciones precisas para conectar a Internet a través de números 900.

Ambas prácticas eran tan viejas como las BBS e Internet. Por ejemplo, la denuncia contra Isla Tortuga se había basado en los cracks que se ofrecían, pero lo que había allí a montones eran números de tarjetas de crédito, robados o generados con programas especializados. En cuanto a los 900 se conseguían probando uno a uno, de forma automatizada, rangos de números de teléfono hasta encontrar los gratuitos.**[56]**

Para ello era útil trabajar en equipo, normalmente dentro de un mismo grupo de hackers, ya que se repartían los rangos a escanear:

> Por ejemplo "yo esta semana escanearé los 900354xxx" y él los 900355xxx y aquella semana escaneábamos aquellos rangos (2.000 números) y después nos avisábamos de en qué números atendía un módem. Y a la semana siguiente, otros rangos. Así encontramos muchos 900, especialmente en los rangos 90035xxxx.**[57]**

Por aquel entonces, muchas empresas tenían números 900 para que sus empleados pudiesen mandarles datos (por ejemplo el périto de una aseguradora) o para centralitas. Una de estas empresas era Recoletos, editora de medios de comunicación como "Marca" o "Expansión". Un hacker que trabajaba allí filtró uno

de los números al “underground”, lo que en menos de un año conllevó facturas de teléfono de varios millones de euros a la empresa, que acabó cerrando aquella línea.

Cuando un phreaker localizaba un 900 se lo quedaba para uso propio o lo regalaba a los amigos; pero en este último caso siempre acababa habiendo filtraciones que hacían correr el número por todo el “underground”, en listas de correo, canales de IRC o foros en la web. Cuanto más privado se conservaba el número, más tiempo se podía usar, incluso años, porque las facturas no alertaban a la empresa. Divulgarlo era “quemarlo”:

> La multinacional SITA, relacionada con la industria aeronáutica, tenía una pasarela X25 a través de un número 900 que alguien filtró. Pero para entrar a X25 se necesitaba también una Network User Address (NRI). Alguien lo simplificó con un programita que conectaba a SITA y después a los NRI. Pero claro, el problema de hacer las cosas sencillas es que los script_kiddies se aprovechan, y después cierran los 900 y vienen las denuncias.**[58]**

La mayoría de empresas que descubrían que los hackers estaban usando sus módems gratuitos cerraban la línea y ya está. Pero algunas lo denunciaban. Fue el caso, en 1997, de IBM Global Services. Pero no afectó a tanta gente ni tuvo la trascendencia mediática de la Operación Millenium.

En su nota de prensa, hoy desaparecida, la Guardia Civil calificaba la operación como el “descubrimiento de una de las redes más importantes de defraudadores en nuevas tecnologías”. Sabiendo cómo funcionaba el descubrimiento y circulación de números 900 en la red, esta afirmación era incierta, aseguraba el investigador Bernardo Quintero, de Hispasec:

> Hemos podido constatar que los números 900 motivos de la investigación estaban al alcance en diversos foros, sin necesidad de pertenecer a un grupo determinado para acceder a ellos. Parece claro que no existía un grupo organizado tan voluminoso y que este y otros aspectos sobre la operación se han podido sobredimensionar en los diferentes comunicados.**[59]**

La mayoría de acusados, estudiantes de Informática o Telecomunicaciones, aseguraron no tener relación con COM 30 y haber encontrado los números en Internet, donde era fácil localizarlos, como corroboraron los medios:

> La utilización fraudulenta de los números 900 era un secreto a voces en Internet, donde se pueden encontrar numerosas listas de dichos dígitos para que los usuarios los utilicen a su libre albedrío.**[60]**

Cuatro años después, la mayoría de sentencias fueron absolutorias**[61]**. En bastantes casos, las denuncias ni siquiera prosperaron, por defecto de forma: bien por mala redacción o porque la cantidad de dinero que supuestamente habían gastado no llegaba a las 50.000 pesetas y por tanto no era fraude.

Según el abogado Carlos Sánchez Almeida, quien defendió a tres detenidos, entre ellos a _X_, la Operación Millenium significó un jarro de agua fría para el “underground” hispano:

> Fue la operación policial que generó más paranoia, mucho más que el caso !Hispahack, por el

> número de implicados y porque todo el “under” usaba estos números.[62]

A partir de estos hechos, algunos grupos de hackers abandonaron su actividad y otros restringieron mucho la admisión de nuevos miembros, como recuerda uCaLu, de Undersec, porque se sospechaba que había habido un delator:

> Después de la operación Milenium volvió a entrar el pánico en los grupos nacionales de hack/phreak/virus … y se hermetizo de nuevo todo, ya que muchos de nosotros pensábamos que el descubrimiento de los patanes de la Guardia Civil no habían sido por ser técnicamente buenos… sino por chivatazos. Por lo tanto se volvió a la época en la que era muy difícil formar parte de grupos de Hack para los que empezaban en ese momento.[63]

La operación Millenium recabó además muchas críticas por considerarse una operación de imagen, un día antes de la celebración de las primeras Jornadas sobre Delitos Cibernéticos de la Guardia Civil, como explica Sánchez Almeida:

> Fue una operación política montada por Mayor Oreja porque coincidía con unas jornadas de seguridad en Madrid y la campaña electoral en marzo de 2000. Aprovecharon esta operación para demostrar eficacia.[64]

5. Notas

1. ↑ Un 'agujero' en La Moncloa. Iñigo More. "El País" (13-10-95)
2. ↑ Obtaining and Cracking a UNIX Password File (Part 1). Ice Dragon. The Information Warfare Site
3. ↑ ABC demuestra la inseguridad informática de los principales organismos del estado. J.M. Nieves, R. García, A. Rodríguez. "ABC" (29-09-96)
4. ↑ Los rescatadores. Mercè Molist para "Ciberpaís" (18-04-01)
5. ↑ "Soy totalmente contrario a contratar hackers". Entrevista Carlos García. Mercè Molist
6. ↑ "Los hackers son un poco autistas". Entrevista Anselmo del Moral. Olalla Cernunda y Pedro de Alzaga. "El Mundo" (06-11-98)
7. ↑ Detienen a un joven de Murcia, acusado de robar ficheros en un ordenador del Ministerio del Interior, por Internet. Mercè Molist (1999)
8. ↑ Un juez archiva el caso del 'hacker' de Interior y afirma que acceder a una 'web' no es delito. "El País". *Ciberpaís* (16/05/02)
9. ↑ Mave, en conversación privada
10. ↑ Mave, en conversación privada
11. ↑ Mave, mensaje privado a KHK (01-96)
12. ↑ Lester, en conversación privada
13. ↑ Mave, en conversación privada
14. ↑ Mave, mensaje privado a KHK
15. ↑ Primer caso contra "ciberintrusos". Olalla Cernuda. Diario del Navegante. "El Mundo" (13-05-99)
16. ↑ Se busca Ciberdelincuente. Rosa Infante. "El Mundo" (01-03-98)
17. ↑ "Los hackers son un poco autistas". Entrevista con el teniente Anselmo del Moral, jefe del Grupo de Delitos Informáticos de la Guardia Civil. Olalla Cernuda. Diario del Navegante. "El Mundo" (06-11-98)
18. ↑ Hackers. Emilio del Peso Navarro. IEE Informáticos Europeos Expertos. Revista "En Línea" n.16 (11-97)
19. ↑ Primer caso contra "ciberintrusos". Olalla Cernuda. Diario del Navegante. "El Mundo" (13-05-99)
20. ↑ Se busca Ciberdelincuente. Rosa Infante. "El Mundo" (01-03-98)
21. ↑ Apuntes del sumario. Mercè Molist
22. ↑ Primer caso contra "ciberintrusos". Olalla Cernuda. Diario del Navegante. "El Mundo" (13-05-99)
23. ↑ El fiscal pide el indulto para los presuntos 'hackers' de Tarragona. Mercè Molist (10/05/00)
24. ↑ El fiscal pide el indulto para los presuntos 'hackers' de Tarragona. Mercè Molist (10/05/00)
25. ↑ Apuntes del sumario. Mercè Molist
26. ↑ La seguridad informática entra en juego. Mercè Molist para "Ciberpaís" (20-02-00)
27. ↑ Los incidentes de seguridad se doblan en un año. Mercè Molist para "Ciberpaís" (16-01-01)
28. ↑ Los ataques informáticos subieron moderadamente el año pasado. Mercè Molist para "Ciberpaís" (09-01-03)
29. ↑ Hispahack: tres "cerebros" desactivados. Mirta Drago. Diario del Navegante. "El Mundo" (04-04-98)
30. ↑ El informe pericial del esCERT añade nuevos datos al "Caso Hispahack"*. Mercè Molist para "Ciberpaís"*
31. ↑ Jordi Murgó, en conversación privada
32. ↑ El informe pericial del esCERT añade nuevos datos al "Caso Hispahack"*. Mercè Molist para "Ciberpaís"*
33. ↑ El informe pericial del esCERT añade nuevos datos al "Caso Hispahack"*. Mercè Molist para "Ciberpaís"*
34. ↑ *Los 'ciberpiratas' españoles se cuelan en la NASA y el Pentágono*.J.G.Albalat. "El Periódico de Catalunya" (01-06-98)

35. ↑ Web del congreso hackeada. Noticias Underground. JJF HACKERS TEAM JOURNAL 01 (1997)
36. ↑ Yandros, cofundador de Hispahack, en conversación privada
37. ↑ Los 'men in green' del capitán moral.es. *Luis Gómez. "El País" (19/03/00)*
38. ↑ Diario de Sesiones de Comisión Especial sobre redes informáticas del Senado, número 488 de fecha 30/09/1999
39. ↑ Diario de Sesiones de Comisión Especial sobre redes informáticas del Senado, número 488 de fecha 30/09/1999. Anselmo del Moral.
40. ↑ Salvado por el nick. Mercè Molist para "Ciberpaís" (10-06-99)
41. ↑ Absuelto el acusado del "caso Hispahack!". El Mundo (04-06-99)
42. ↑ Sentencia Caso !Hispahack (28-05-99)
43. ↑ Salvado por el nick. Mercè Molist para "Ciberpaís" (10-06-99)
44. ↑ En la hora de la victoria. !Hispahack
45. ↑ Caso !Hispahack: La Resolución del juez
46. ↑ Sentencia Caso !Hispahack (28-05-99)
47. ↑ En la hora de la victoria. !Hispahack
48. ↑ *Los ciberpiratas españoles se cuelan en la NASA y el Pentágono*. J.G. Albalat. "El Periódico de Catalunya" (01-06-98)
49. ↑ "Todo ha sido un montaje policial". *Ángel Cortés. Noticias.com (08-04-98)*
50. ↑ Carlos Sánchez Almeida, en conversación privada
51. ↑ Yandros, cofundador del grupo, en conversación privada
52. ↑ Fermín J. Serna (Zhodiac), en conversación privada
53. ↑ Operación "Millenium": las dos caras de la moneda. Bernardo Quintero. Hispasec (17/01/00)
54. ↑ Detenidos cien internautas de 16 provincias por una estafa informática. Mercè Molist. El País (19/01/00)
55. ↑ Operación "Millenium": las dos caras de la moneda. Bernardo Quintero. Hispasec (17/01/00)
56. ↑ Líneas 900. Jeck's page (1998)
57. ↑ Anónimo
58. ↑ Anónimo
59. ↑ Operación "Millenium": las dos caras de la moneda. Bernardo Quintero. Hispasec (17/01/00)
60. ↑ La Guardia Civil detiene a un centenar de personas por utilización fraudulenta de "números 900". *Olalla Cernuda. "El Mundo" (18/01/00)*
61. ↑ Así terminan las redadas de hackers. HackHispano (05/04/04)
62. ↑ Carlos Sanchez Almeida, en conversación privada
63. ↑ uCaLu, en conversación privada
64. ↑ Carlos Sánchez Almeida, en conversación privada

6. Enlaces externos

· Maderos del siglo XXI. Mercè Molist.
· Diez años "apatrullando" la red. Mercè Molist para "Ciberpaís" (11-05-05).
· Entrevista Chelo Malagón. Mercè Molist para "@rroba" (15-11-05)
· El fin de la inocencia de la inseguridad informática. Mercè Molist para "Cibepaís" (28-01-08)
· Empieza a tomar forma la red de CERTs españoles. Mercè Molist para "Ciberpaís" (25-04-07)
· La hora de los hackers. Carlos Sánchez Almeida. Conferencia impartida en el marco del IV Ciclo de Conferencias UPM TASSI 2010 (27-04-10)

6.1. Universitat Rovira i Virgili

· Escasa acogida en la primera reunión de los internautas catalanes. "Computerworld" (06-12-96)
· TINET, la Xarxa Ciutadana de les comarques de Tarragona. Tarraco Wiki.
· Entrevista Chelo Malagón de IRIS-CERT. Mercè Molist para "@rroba" (15-11-05)
· Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet. Andreu Veà Baró. Tesis Doctoral (12-09-02)

6.2. El caso Hispahack

· Especial 'Caso !Hispahack'
· Mi punto de vista. *Net Savage*
· El ataque de "Hispahack". *Jan Martínez Ahrens. "El País" (04-04-98)*
· Caso Hispahack (1): Absolución de presuntos hackers. La sentencia
· Caso Hispahack (2): Absolución de presuntos hackers. Informe final de la defensa
· Caso Hispahack (3): Absolución de presuntos hackers. Dictamen del perito de la defensa
· Notas del juicio a JFS. Mercè Molist (26-05-99)
· Hispahack: tres «cerebros» desactivados, *El Mundo (04-04-98).*
· Los detenidos por pirateo informático denuncian un montaje policial, *El País (05-04-98).*
· Asalto a La Moncloa, *El Mundo (15-08-99).*

6.3. Operación Millenium

· Caso Millenium. Delitosinformaticos.com (07/03/05)
· Tercer absuelto del 'Caso Millenium', que causó una gran redada en el año 2000. "El Mundo" (01/03/05)
· Caso Millenium (1): no concurre prueba concreta del proceso de defraudación. Almeida Abogados Asociados (14-02-05)
· Caso Millenium (2): la titularidad de una línea no presupone autoría delictiva. Almeida Abogados Asociados (30-03-04)
· Caso Millenium (3): absolución por presunto phreaking. Almeida Abogados Asociados (30-10-03)

CAPÍTULO SIETE

Sudo apt-get install anarchy

Sudo apt-get install anarchy

DECLARACIÓN DE INDEPENDENCIA DEL CIBERESPACIO

Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos.

No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquella con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente.

(...) No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

(...) Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento. Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o el conformismo.

Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia. Aquí no hay materia. (...) En nuestro mundo, sea lo que sea lo que la mente humana pueda crear puede ser reproducido y distribuido infinitamente sin ningún coste. El trasvase global de pensamiento ya no necesita ser realizado por vuestras fábricas.

Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes.

John Perry Barlow. Davos, Suiza. 8 de febrero de 1996.[1]

1. La comunidad libre

El movimiento del software libre aparece a mediados de los 90, cuando el sistema operativo GNU/Linux encandila a geeks de todo el mundo, especialmente en Europa.



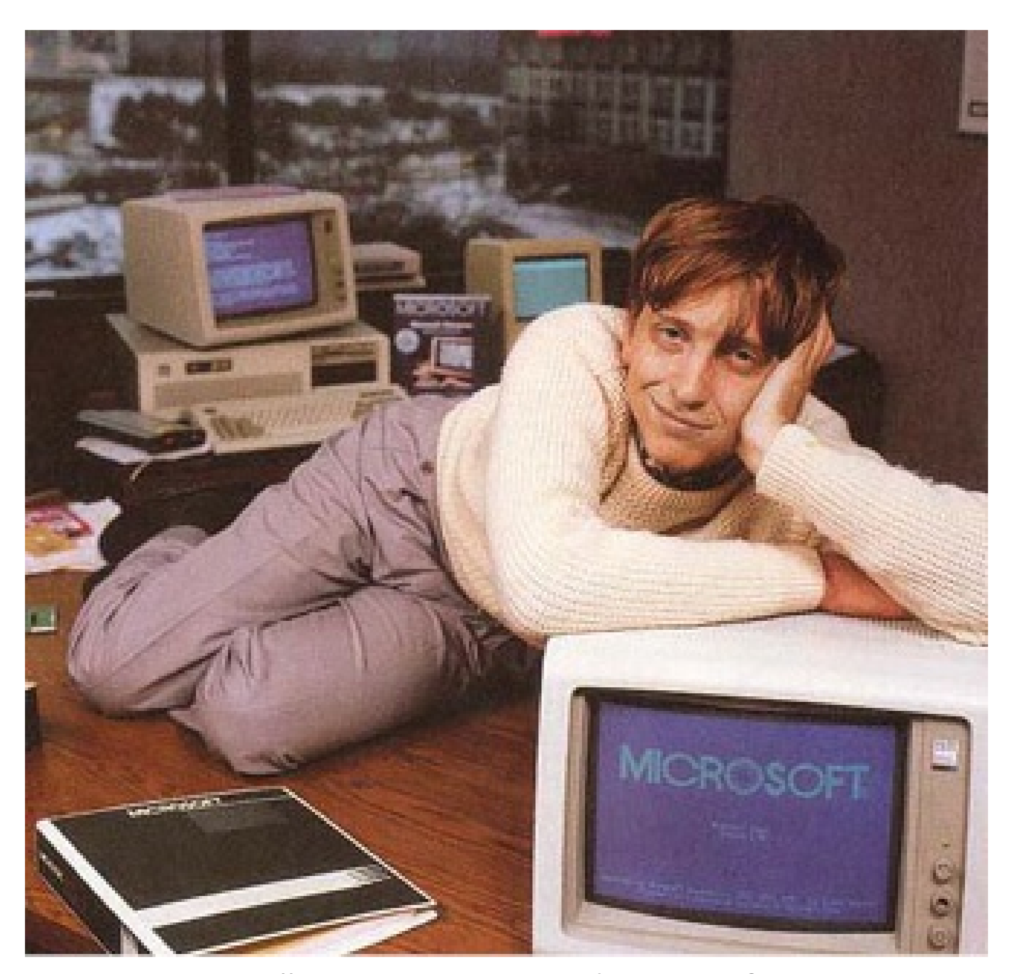
Richard Stallman, disfrazado de San IGNUcio

Richard Stallman inició el movimiento de creación de programas libres en 1984, con el nombre GNU. Cuenta la leyenda que Stallman trabajaba en el Laboratorio de Inteligencia Artifical del MIT (Steve Levy le llama en su libro Hackers, heroes of the computer revolution *"el último hacker auténtico"*. Un día, se estropeó una impresora y Stallman, acostumbrado a trabajar con programas abiertos, buscó el código fuente del controlador, para localizar el fallo.

Pero era un programa comercial y de código cerrado a cal y canto. Así que Stallman llamó a la empresa que lo había vendido a la universidad para que le mandasen el código fuente. La empresa se negó y provocó con ello la ira de Stallman[2], quien juró no volver a usar programas propietarios.

La reacción de Stallman se entiende en el contexto de la primera generación de hackers, ya que todos los programas que crearon eran de código fuente abierto y otros podían leerlo, modificarlo y compartirlo. De hecho, si la World Wide Web hubiese sido de pago, Internet no sería lo que es. Bill Gates fue el primero que vendió un programa, BASIC de Altair, que algunos aseguran que ni siquiera escribió.

Y aquí empezó el negocio del *software* y el odio de los hackers *auténticos* contra Gates.



Bill Gates, promocionando Microsoft

En 1983 Stallman anunció a la comunidad de Internet la puesta en marcha del proyecto GNU, con la intención de crear un sistema operativo totalmente libre. Pero Stallman no sólo tuvo la idea, también diseñó una manera óptima de ponerla en práctica que fue la auténtica revolución: las licencias **copyleft**.

> Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Inglés como copyleft (lo cual significa que el autor permite la distribución libre del mismo, en clara oposición a copyright -'derecho de autor'-), y está contenida en la Licencia General Pública de GNU (GPL).[3]

En 1985 se creaba la Free Software Foundation para dar soporte legal, logístico y financiero a la idea y algunos selectos *geeks* repartidos por todo el mundo empezaron a escribir código para el proyecto. Hasta que, en 1991, el finlandés Linus Torvalds, informa a la comunidad de que está trabajando en un *kernel* o núcleo libre.

De aquí nace el sistema operativo GNU/Linux, la pieza que le hacía falta al proyecto, pues aunque ya se había creado bastantes programas faltaba un núcleo que funcionase tan bien como Linux. Casi al mismo tiempo, en 1993, aparece otro sistema operativo: FreeBSD, fuera del proyecto GNU pero con código de la Free Software Foundation. Los seguirán muchos otros proyectos, en lo que Eric S.

Raymond llamará *“la venganza de los hackers”*.

Efectivamente, el software libre seduce a cada vez más hackers mientras avanza la década de los 90. No sólo les gusta por ideología o por el placer de tener un sistema que pueden manejar a su antojo. Está también el detalle de que Linux se basa en Unix y ya no habrá que andar asaltando sistemas Unix en la red para disfrutar tocando código: ahora es tan fácil como instalar en el ordenador de casa una Red Hat (uno de los “sabores” de Linux) o una Suse o una Debian.



Cabe decir que usar software libre no será tarea fácil al principio. El proyecto se está construyendo sobre la marcha, está todo en inglés, no hay manuales, a veces ni siquiera programas o controladores para según que *hardware*, que se ha construido pensando sólo en el omnipresente sistema operativo Windows. Es un grave problema no sólo para el usuario normal sino también para el hacker y la solución pasa por escribir más código, generar más documentación y crear comunidades donde ayudarse los unos a los otros.

“Aquí la comunidad empezó en las universidades, donde se usaba mucho software GNU, pero la gente estaba en grupos internacionales. En 1991 creamos la lista de correo *PDSoft* (Public Domain Soft). La segunda ola llega con Linux, en 1995, cuando entra también gente de las BBSs y aparecen muchos grupos”, explica **Jesús M. González-Barahona**, fundador de *SoBre*, activa asociación para la promoción de los programas libres.[4]

No hay ni ha habido aventura en la comunidad hacker donde se haya realizado una tarea tan ingente de apostolado como con el software libre. Paco Brufal desde el

área de Fidonet R34.LINUX, el foro más antiguo sobre Linux, Jesús González-Barahona desde la Universidad Carlos III, Ismael Olea y Juan José Amor desde la Asociación Hispalinux y el Proyecto LuCAS de traducción de manuales, Antonio Castro, **Enrique Zanardi** y **Luis Colorado**, del Grupo Español de Usuarios de Linux (SLUG), Jesús Rodríguez del Proyecto FreeBSD, Amaya Rodrigo, la primera mujer desarrolladora de Debian en Europa[5], fueron nombres destacados en aquella tarea ingente de enseñar al que no sabe, donde había comprometidos proyectos que representaban a muchísima más gente: el metablog de noticias Barrapunto, la lista de correo *l-linux*, el canal de chat *#linux*, el proyecto de traducción de páginas de manual PAMELI, es.comp.os.linux, *Spanish GNU*, el proyecto de traducción de COMO's y otros documentos cortos INSFLUG...

Todos esos grupos, iniciativas, servicios de información, repositorios de programas, listas de correo, grupos de noticias o canales de IRC estaban fervientemente ocupados en la traducción de manuales al castellano, dar ayuda técnica y formar y cohesionar a la comunidad. Una comunidad altamente organizada, con todos los servicios que necesitaba: se charlaba en es.comp.os.linux, se bajaban los manuales en PAMELI, las FAQ en LuCAS, Hispalinux montaba congresos.... En todos los rincones de esta comunidad se sentía la revolución, festiva y deliciosamente caótica, fragmentada y a la vez unida en los distintos grupos, a veces armónicos, a veces enfrentados, como la vida misma. En 1999, la versión 3.0 del Proyecto LuCAS superaba las 100.000 visitas, el software libre era motivo de charlas y congresos en todas partes, donde siempre se incluía una install party.

Las *install parties* eran una genial idea para superar el principal miedo del novato: instalar en su ordenador un sistema operativo desconocido que además, en los 90, no era tarea fácil. Se aprovechaba cualquier congreso, sesión de charlas, fiesta, lo que fuera que tuviese que ver con la informática para "colar" una *install party*. Según comenta Javi Espejo, quien montó bastantes, se hicieron más de mil en toda la geografía española.[6]

Ayudando en todas estas tareas de promoción del software libre estaban los Grupos de Usuarios Linux (LUGs en inglés), asociaciones de difusión y apoyo a los usuarios, creadas en base a la geografía: ciudades, provincias, comunidades autónomas, países, pero no necesariamente. Uno de los grupos de usuarios más importantes de España fue el de Mallorca.

1.1. Bisoños usuarios de GNU/Linux

La comunidad hacker de las Illes Balears era muy fuerte. Se vertebraba alrededor de la asociación y grupo local de usuarios BULMA (Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons | Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores). Su creador fue *DrSlump*.

> Bulma nace en 1998 gracias al actual presidente, Javi Polo, quien después de asistir al congreso de Hispalinux se le ocurrió montar un grupo de linuxeros. En la primera reunión sólo eran 18 socios.[7]



El buen hacer de los primeros integrantes de BULMA y la ayuda de personas de la Universitat de les Illes Balears (UIB) hicieron que el grupo creciese rápidamente y se crease una nutrida comunidad virtual, cuyo principal punto de reunión era la lista de correo Bulmailing.

Esta comunidad trascendió pronto el entorno de les Illes Balears, extendiéndose a toda Catalunya y más allá. Así surgió en Barcelona el grupo afín Badopi (Barceloneses Domadores de Pingüinos/Barcelonins Domadors de Pingüins), centrado en la lista de correo Comando B. Javi Polo estaba entre sus creadores:

> Hacía poco que me habia mudado a vivir a Barna, y como en la lista (Bulmailing) en esa epoca habia gentes de todos lados, alguien se pispó de que habia mucha gente de por aqui , y Oriol Raventós propuso de hacer una kdd de la lista de bulma en barna, en diciembre de 2002. La primera cena aparte de un éxito de asistencia fue un éxito en cuanto al elenco de personajes que nos juntamos, todos (menos uno) unos cracks muy motivados. El grupo se consolidó sin mucho esfuerzo … y con muchas risas.[8]

Uno de los hackers que pululaban por Badopi fue José Luís Maquieira, quien musicó en 2003 la Canción del software libre, que acabó siendo el *Himno de Badopi*.

1.1.1. La Canción del Software Libre

La Canción del software libre (Alberto García González) fue una adaptación de un tema de Marc Parrot, que la compañía de telefonía móvil Amena usó en su campaña publicitaria de lanzamiento. El tema de Parrot era a su vez una adaptación de la canción "Libre" de Nino Bravo.

En 1999, el anuncio de Amena y su pegadizo *jingle* sonaban insistentemente en televisiones y radios, siendo el caldo de cultivo para que Alberto García González (*Berto*) re-adaptase la re-adaptación. Había nacido la *Canción del software libre*.

> Tenía un amigo al que le encantaban los chistes y los juegos de palabras. Ambos estudiábamos informática, y Linux se había puesto bastante de moda en el mundillo. Un día por la mañana yo estaba tarareando la melodía y me salió lo de "como el código de Linux yo soy libre", a lo que él respondió "como el taaaar". Siguiendo con la broma completamos el estribillo en cuestión de minutos, y la cosa terminó ahí. Después pensé que, como el chiste había quedado gracioso, valía la pena completar la canción y publicarla.[9]

Berto la mandó a Fidonet y la canción empezó a correr por el ciberespacio hasta que, en la Navidad de 2003, José Luís Maquieira y un amigo músico grabaron una interpretación de la misma, que ofrecieron libremente en Internet. El tema fue un éxito en la comunidad linuxera.

El mensaje original que mandó Berto a Fidonet fue este:

```
From: Alberto Garcia Gonzalez
Date: Tue, 09 Nov 1999 21:43:48 +0000
Subject: Libre

   Ahi va una apologia del software libre a ritmo de Nino Bravo.
Espero que os mole, no me abucheéis mucho:

----->< ----->< -- Corta por aqui --><----->< -----
Libre
-+-+-

Lleva apenas veinte horas y ya está
buscando un Service Pack
Porque le soltó una pantalla azul
el Visual C++

Luego navegando por la World Wide Web
lo vio con claridad
un compilador llamado GCC
rezaba sin parar


(ESTRIBILLO)
Libre, como el código de Linux yo soy libre
como el tar
Libre, como el bison, como el perl y como el cron
que puedes compilar
Libre, como Debian que me ofrece herramientas sin pagar
también tengo Red Hat
que viene con manual
ahora si sé lo que es la libertad


El código abierto es su nueva fe
programa en GTK
ahora es un tipo muy muy popular
en la lista de Bugtraq

Estaba tan harto de usar NT
que decidió cambiar
ya maneja Linux y FreeBSD
en cualquier terminal

(ESTRIBILLO)
-----><-----><-- Corta por aqui --><-----><-----
```

1.1.2. La Balearikus Party

Junto con Javi Polo, el resto de fundadores de BULMA la fueron abandonando debido, según la versión de los que se fueron, a la mayor implicación en la comunidad del profesor de la UIB Ricardo Galli, quien años después pondría en marcha, junto con el informático Benjamí Villoslada, el famoso metablog Menéame. Galli estaba con BULMA desde sus inicios:

> El servidor era de un proyecto de investigación mío, porque ellos me ayudaron a instalar “en secreto” los GNU/Linux que usé para clase en la UIB y era mi gran deuda con esos chicos. El software de bulma.net, desarrollado inicialmente por Antonio Tejada Lacaci, fue luego desarrollado y mejorado prácticamente por mí solo.[10]

Los problemas del equipo fundador con Galli llegaron cuando éste fue elegido presidente, explica Polo:

> Cuando Ricardo empezó a inmiscuirse más en Bulma se empezaron a polarizar bastante las cosas entre los seguidores incondicionales de Galli y los no incondicionales y se enrareció todo bastante.[11]

Benjamí Villoslada, quien también estaba en BULMA, tiene otra versión:

> En realidad Ricardo protagonizó el esplendor de BULMA. Los rebotados fueron anécdota. Todo subió con él muchas magnitudes.[12]

Y Galli:

> Durante mi participación activa en Bulma (de 2001 hasta principios de 2004) Bulma vivió sus mejores años en número de participantes en la lista, artículos en el web (y desarrollo del mismo), proyectos, conferencias... artículos de bulma.net que salieron en Slashdot, algunos de ellos traduciones al inglés, otros publicados en revistas internacionales, organizamos conferencias donde traíamos a personas relevantes. La lista empezó a decaer en 2005, cuando yo ya no participaba.[13]

Uno de los mayores logros de BULMA, ayudada por la UIB, fue la Balearikus Party, una LAN-Party que nació en mayo del 2000, como actividad paralela a la jornada de puertas abiertas de la UIB[14].

> Se montó una red de 70 ordenadores traídos por los participantes, en la que por el éxito inesperado no pudimos dar sitio a todas las demandas, agotándose en pocos días las plazas que habíamos anunciado.[15]

En la segunda edición, en 2001, se pasó de 70 equipos a 400. Y se incluyeron conferencias donde hablaron Ricardo Galli y su mentor, el catedrático en ciencias de la computación e inteligencia artificial de la UIB Llorenç Valverde. Hubo también organizadores de la No cON Name dando charlas: Nico Castellano, Javier Olascoaga y Simon Roses[16]. La Balearikus se celebró anualmente hasta 2008.

1.2. Es.comp.os.linux

Si hablamos de la historia del software libre en España es obligado mencionar el que fue su centro neurálgico: el grupo de noticias es.comp.os.linux, que nació en agosto de 1996, a iniciativa de Pablo Saratxaga.



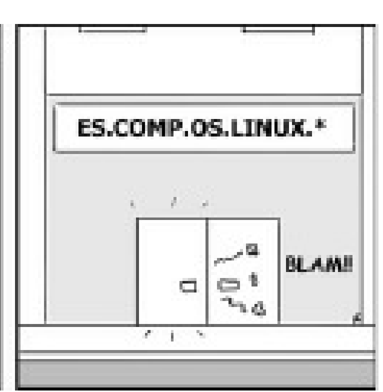
Es.comp.os.linux creció mucho en poco tiempo y generó nuevos puntos de encuentro, pequeñas comunidades dentro de la gran comunidad, entre ellas grupos de noticias más especializados que colgaban del primero, como es.comp.os.linux.programacion o es.comp.os.linux.redes[17], el canal #escomposlinux en el IRC-Hispano y una lista de correo de traducción de documentación y programas libres a los idiomas del estado español[18].

El proyecto global se llamó es.comp.os.linux.* y aún sigue en pie su sitio web http://www.escomposlinux.org, sufragado y soportado por voluntarios desde el año 2000, de forma altruista.[19]

Es.comp.os.linux.* fue un ejemplo nítido de cómo funciona una comunidad hacker: ante todo con humor[20] pero poca gente haciendo el cafre. Eran hackers del código[21], hijos directos de la primera generación, comprometidos con la popularización del software libre, que se tomaban muy en serio. Hackers impecables en su ética.







A la guardería!. Javier Malonda (15-11-01). [ampliar]

Los más brillantes nombres del movimiento del software libre y algunos de la comunidad hacker española entran y salen de la historia de es.comp.os.linux.*. Sólo hay que ver la lista de colaboradores habituales del proyecto, entre ellos **Mauricio Saint-Supéry**, **Iñaki Arenaza**, **Benjamín Albiñana**, **Andrés Herrera**, **Santiago Benejam**, **Javier Cantero**, **Jesús Carrete Montaña**, **José Antonio Calvo** y etc. O los que votan a favor de la creación de los diferentes grupos de noticias de es.comp.os.linux: Ismael Olea y Juan José Amor, líderes del Proyecto Lucas[22], **Modesto Garrido**, **Antonio Pardo**, **J.A. Gutierrez**, **Xavier Caballé**.[23]

El mayor esplendor del grupo de noticias es.comp.os.linux se vivió entre 1996 y 2002, aunque hubo circulación de mensajes hasta 2006. Este y sus hermanos fueron grupos modélicos, siempre poblados, con mensajes interesantes y prácticamente libres de spam gracias a que un par de colaboradores del proyecto, Benjamín Albiñana y, más tarde, Jesús Carrete, crearon filtros para parar esa lacra no sólo en los grupos de Linux sino en todos los grupos de noticias de la jerarquía es.*.

1.2.1. La tira ecol

Es obligado destacar la aportación a la comunidad linuxera hispana del ingeniero **Javier Malonda**: La Tira Ecol, una tira cómica semanal que nació en 2001, sobre las peripecias de Bilo y Nano, dos “freaks”, compañeros de piso, el uno experto en Linux y el otro, usuario de Windows.

> “La idea no fue mía. Un día, comiendo con Santiago Romero, se le ocurrió que podría dibujar algo sobre el grupo de noticias es.comp.os.linux, en el que participábamos activamente. La popularización de la tira coincidió con el inicio del proyecto EcolNet (Ecol son las iniciales de es.comp.os.linux) y ahí se hospedó. Bilo y Nano no habrían llegado a ninguna parte sin ellos”.[24]



Mandriva. Javier Malonda (07-04-05). [ampliar]

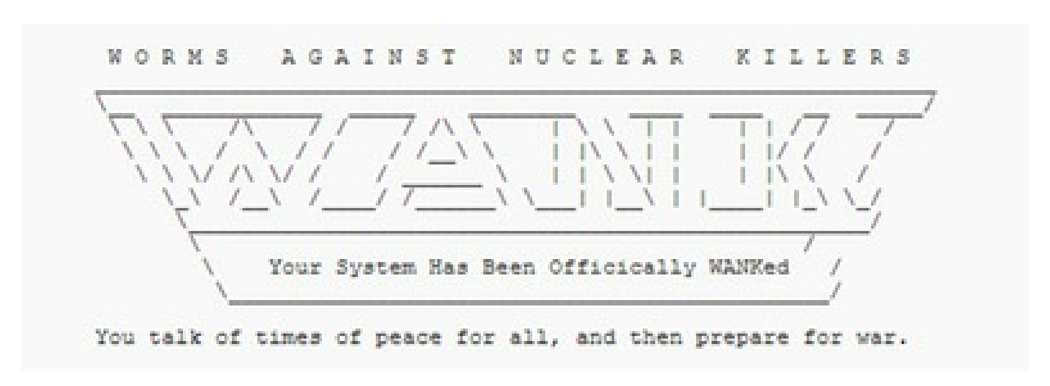
La Tira Ecol fue muy popular y traspasó las fronteras de la comunidad Linux. Muchos blogs la replicaban. Se tradujo, totalmente o en parte, al inglés, francés, catalán, gallego, euskera, italiano y aragonés. Sólo la edición en castellano tenía, a finales de 2003, 10.000 visitas. 4.000 la catalana. Se publicó hasta 2012.

> “Atribuyo gran parte del éxito a su licencia libre, que le permite ser distribuida y enlazada en todas partes, sin restricciones ni pedir permiso”.[25]

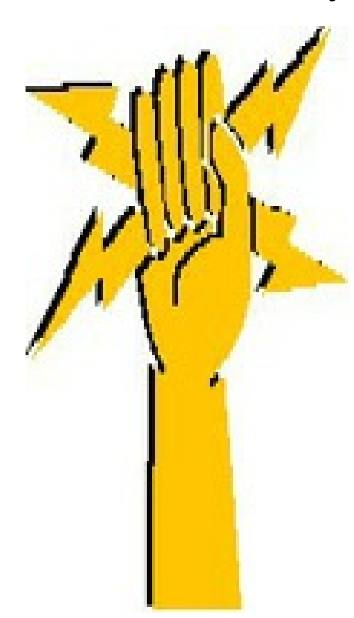
2. La comunidad hacktivista

Hacktivismo significa hacer hacking por una motivación política o social. Cabe decir que, en los inicios de este movimiento, la palabra *hacktivismo* no existía. La popularizó el grupo Cult of the Dead Cow en 1999[26]. Mientras, en vez de hacktivismo se hablaba de net-activismo o cíberactivismo.

El primer caso conocido de hacktivismo en las redes se remite a octubre de 1989, cuando un virus del tipo gusano penetró en las máquinas VAX de las redes del DOE (Departamento de Energía norteamericano), HEPNET (Red de Física de Alta Energía) y SPAN (Programa de la NASA). El gusano, llamado **WANK**, cambió el mensaje de entrada a estos sistemas por otro antinuclear:



Los creadores de virus han sido bastante dados a usar sus criaturas para reivindicaciones, como el virus *Anti-Tel* del grupo catalán **Los Dalton**, que en 1991 se quejaba de las elevadas tarifas de Telefónica. O el *Anti-ETA* creado por **GriYo** de 29A en 1998, como protesta por el asesinato del concejal del PP Miguel Ángel Blanco.



La mano agarrando dos rayos era un símbolo muy usado en la lucha por los ciberderechos

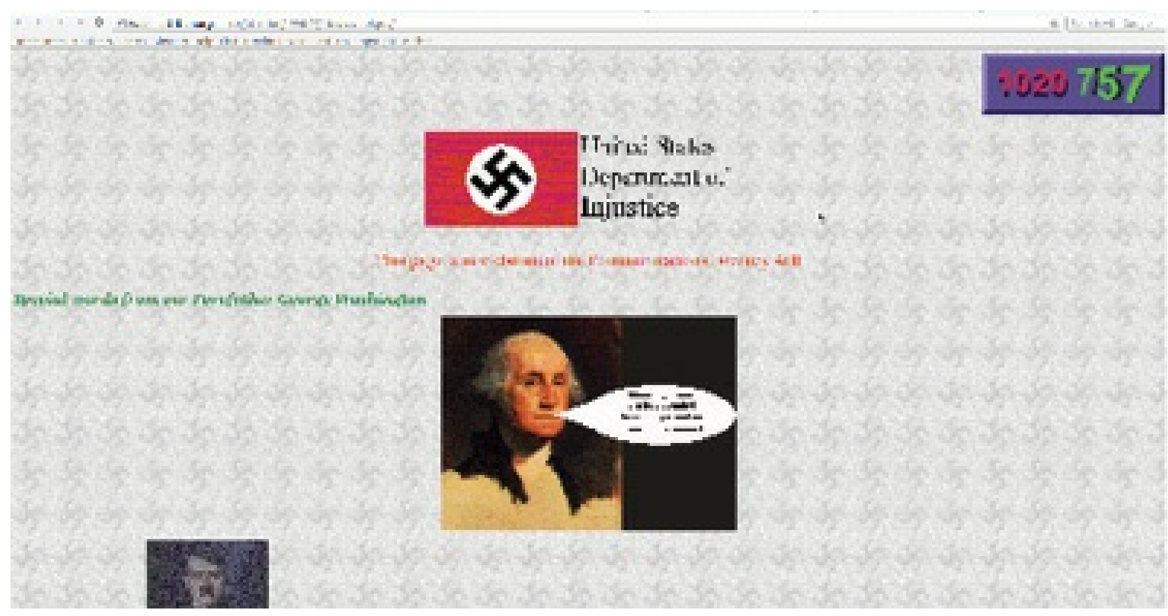
Un paso más allá de los virus fueron las manifestaciones virtuales o netstrikes, un invento de la comunidad hacker italiana que organizó la primera en 1995, contra ordenadores del gobierno de Francia, en protesta por las pruebas nucleares en el atolón de Mururoa. Una manifestación virtual consiste en visitar muchas veces, muchas personas, una página web, hasta conseguir ralentizar o bloquear el acceso a la misma. Los organizadores de esta primera netstrike fueron **Los Anónimos**, **Strano**

Network e **Isole Nella Rete**.

La idea se exportó rápidamente al mundo mundial[27] y en 1996 los norteamericanos y mexicanos del grupo Electronic Disturbance Theatre (EDT), adalides del llamado **zapatismo digital**, la estaban usando contra ordenadores del Pentágono y el gobierno mexicano.

Era cuestión de tiempo que se automatizase la netstrike, haciendo muy fina la frontera entre manifestación y bombardeo: en 1997, EDT creó un pequeño programa que mandaba peticiones de forma repetida a una web. Lo llamaron *Zapatista FloodNet*[28] y fue la primera arma hacktivista[29] . Un año después, en el congreso Ars Electronica, EDT hizo una demostración, atacando tres sitios a la vez: la web del presidente mexicano, el Pentágono y la Bolsa de Frankfurt. Los militares norteamericanos respondieron con otro programa, que *freía* los navegadores de los manifestantes[30]. En 1999, EDT liberó el código fuente de FloodNet, en el que se han basado programas similares en todo el mundo.

En España la comunidad hacker repudió las netstrikes por considerarlas ataques de denegación de servicio y, por tanto, bombardeos, destructivos y contrarios a la ética hacker. Lo que sí ha tenido éxito aquí -como en todo el mundo- han sido los defaces, siendo el grupo portugués Toxyn pionero.



Portada de la web del Departamento de Justicia de EEUU defaceada, en agosto de 1996, en protesta por la Communications Decency Act

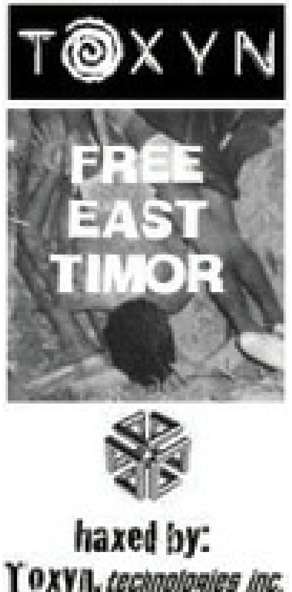
Aunque antes de Toxyn se habían hecho ya en Internet un par de *defaces* con fines reivindicativos, nadie había montado aún una señora campaña que duró meses y meses.

2.1. Toxyn

El grupo portugués T0XyN nació en 1996, liderado por **m0xx**. Son los hackers portugueses más conocidos, debido a la campaña hacktivista *Free East Timor - Free Xanana Gusmão* que llevaron a cabo en 1997-98. La campaña, en defensa de la independencia de Timor Oriental, atacaba servidores conectados a Internet del

gobierno de Indonesia.





Toxyn empezó su campaña afirmando: "Esperamos llamar la atención para la necesaria autodeterminación e independencia de la gente del Timor, oprimida y violada durante décadas por el gobierno de Indonesia. (...) Pedimos tu ayuda para luchar contra la tirania de Indonesia al ocupar el Timor".[31]

El primer ataque fue contra el servidor web del Departamento de Asuntos Exteriores de la República de Indonesia, el 10 de febrero de 1997, que volvió a ser asaltada el 14 de febrero. Vinieron otros ataques a otras webs el 24 de abril, 30 de junio... Para entonces T0xyN había empezado a acompañar cada *deface* con una lista de decenas de servidores gubernamentales y comerciales violados entre *deface* y *deface*.

El 22 de noviembre de 1997, caía la web de la gubernamental Agencia por el Desarrollo y la Aplicación de la Tecnología y lo firmaban **UrBan Ka0s** y **Portuguese Hackers Against Indonesian Tiranny** (P.H.A.I.T.), según el archivo de páginas hackeadas de la revista "2600". En esta ocasión, los 28 servidores atacados al mismo tiempo vieron todos sus datos borrados, incluido el de la Agencia, lo que convierte este ataque en el más destructivo.[32]



La campaña siguió hasta 1998 y, excepto en el ataque del 22 de noviembre, Toxyn se preocupó siempre de no destruir nada que no fuese necesario. Así lo afirmaban en su web:

> No borramos ni destruimos nada, sólo hackeamos sus páginas.[33]

Y lo repetían también en las páginas hackeadas:

> NO hemos destruido ningún servidor. Las páginas originales han sido renombradas. Las páginas index, históricos y logs han sido alterados sólo para nuestra supervivencia. Las organizaciones de hackers afiliadas y administradores de los sistemas involucrados no deben ser considerados responsables.[34]

En el mismo *deface* aseguraban que sus acciones no diferían de una manifestación en la calle:

> Somos como otros manifestantes en las calles, que simplemente tienen la habilidad de poder entrar en estos sitios. Podéis intentar restringir la información, pero la tecnología nos permite ser todos iguales!.[35]

Un año después, se celebró un referéndum de autodeterminación bajo mandato de la Organización de las Naciones Unidas. Timor Oriental fue el primer estado que consiguió la independencia en el siglo XXI, la cual se formalizó el 20 de mayo de 2002.

Diversos hackers ayudaron a Toxyn en su campaña, como el veterano grupo portugués Pulhas. También el hacker catalán Savage, antes The Phreaker en Apòstols, quien creó algunos programas que se usaron para atacar de forma

masiva servidores del gobierno de Indonesia.

> 1996. Conozco a los chicos de ToXyN mientras intentaban hackear algunas máquinas de LleidaNet. Les hago un talk root@ip_del_hacker y nos hicimos coleguillas. (En) 1997, (hago) algunas cosas impublicables, que utilizaron los amigos de ToXyN en la campaña contra Indonesia, por la Independencia de Timor del Este.[36]



Ataque a la red militar de Indonesia, el 24 de abril de 1997

Entre las cosas que hizo Savage para la campaña, destaca un exploit para el servidor de correo IMAP de Linux, que daba acceso total a la máquina atacada y se convirtió en el más popular del siglo XX[37].

Otra creación de Savage para la campaña, que acabó trascendiéndola, fue el programa *QueSO*[38], que determina remotamente sistemas operativos. El popular escáner de seguridad informática Nmap se basó en QueSO. Su autor, Fyodor, se deshace en elogios hacia el trabajo de Savage en la introducción a Nmap[39].

Por cierto que QueSO protagonizó un embrollo memorable de alcance internacional en noviembre de 1998: El proyecto Internet Operating System Counter usaba QueSO para hacer sus estadísticas sobre qué sistema operativos son más populares. Mientras IOSCount recogía datos escaneando ordenadores israelíes con QueSO, desde una máquina llamaba beirut.leb.net, una empresa de seguridad israelí dio la alarma nacional, que ocupó todas las portadas de periódicos con titulares como “Un libanés ataca lugares israelíes en Internet”.[40]

2.2. Nodo50

Otros colectivos han practicado un hacktivismo más pasivo, consistente en dotar de herramientas informáticas, acceso a las redes y alojamiento web a ONGs y grupos alternativos, tarea ardua donde las haya pues la primera reacción de la izquierda ante Internet fue de desconfianza, ya que se consideraba a los ordenadores un instrumento del Sistema.

Este inmovilismo telemático empezó a cambiar en España alrededor de octubre de 1995, cuando debía celebrarse en Madrid una reunión del Fondo Monetario

Internacional y los colectivos anticapitalistas decidieron montar una contracumbre. La ONG madrileña Sodepaz propuso usar Internet para coordinarse, por lo que recurrieron a las dos BBS que destacaban en temas antagonistas: **HELP**, en Barcelona, y **Revolware**, en Madrid,

> Eran pequeños proyectos que aglutinaban a un reducidísimo grupo de “cibermilitantes” y se soportaban sobre sendos ordenadores 286 (uno de ellos “expropiado” en Alemania) con tecnología Fido sobre MS-DOS. HELP estaba soportada por el ímpetu de un solo individuo: **Manolo Barberá**, aunque apoyado muy de cerca por la gente de El Local, la agencia ADAI y GEA, a quien la BBS daba soporte para la difusión de datos de radioactividad post-Chernobil. Por su parte, Revolware surgía de un grupúsculo –con el mismo nombre- dedicado a la crítica y apropiación social de las nuevas tecnologías, y con estrecha relación con la agencia de contrainformación UPA. L@s usuari@s de estas BBSs eran cuatro chalad@s que aunaban su militancia política con el interés por la informática.[41]

Además de estas BBS, había dos proyectos incipientes: IEPALA (Instituto de Estudios Políticos para América Latina y África) en Madrid, respaldado por el profesor de la Universidad Politécnica de Madrid **Joaquín Seoane**, y Pangea en Barcelona, cuya cabeza visible era el profesor de la Universitat Politècnica de Catalunya **Leandro Navarro**. Ambos nacían con la idea de dar servicios telemáticos a ONGs.

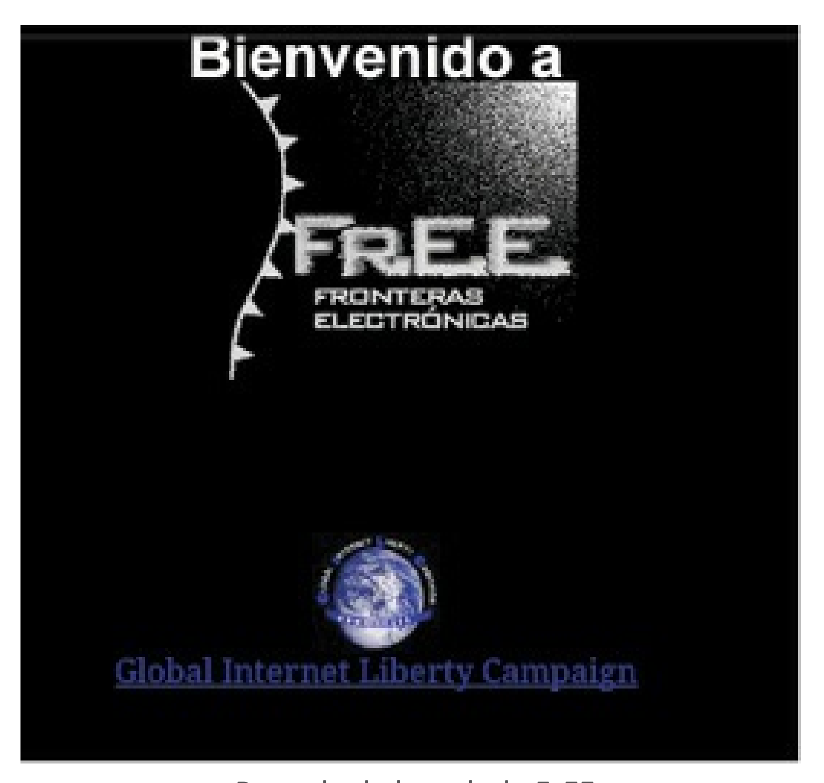
> En torno a (Pangea) se articula una federación de entidades civiles: Comunicació per a la Cooperació, que agrupa al Movimiento de Objeción de Conciencia, Entrepueblos, el Movimiento 0.7% para el Desarrollo y Payasos sin Fronteras. Estos últimos habían descubierto la potencialidad del correo electrónico cuando tras una actuación en el campo de refugiados de Veli Joze, Savudrija, en Croacia, en febrero de 1993, dos voluntarios hicieron llegar un módem y un ordenador, estableciéndose una comunicación telemática en la que pudieron comunicarse niños y niñas del campo de refugiados con alumnos escolares de Cataluña.[42]

La BBS Revolware, con ayuda de gente de GreenNet, tiene listo el servidor para la contracumbre a finales de 1994. Se llamará Nodo50[43] y pronto atraerá a personas interesadas, como **Walter Actis** y **Javier Villate**. Se instala en Bilbao un clon del sistema de Madrid y se conectan, siendo el embrión de la red *Altercom*. Al mismo tiempo, un grupo de Euskal Herria monta, con la ayuda de Nodo50, un sistema similar en Iruñea, que será la primera BBS de la red *Eusnet*.

3. FrEE y las Huelgas por la Tarifa Plana

Junto a Toxyn o Nodo50, cuyo activismo en la red se ha dirigido a defender causas del Mundo Real, la comunidad hacktivista cuenta también con grupos cuya misión es luchar por los habitantes de Internet y sus derechos: los ciberderechos. Esta fue la tarea de la ONG Fronteras Electrónicas de España (FrEE).

FrEE nació en 1996 de la mano de **DA5ID** (David Casacuberta), **Marco13**, **José Luís Martín Más**, **Anabomber** y **Oscar 999**. Procedían de la filosofía ciberpunk y desde 1994 publicaban el fanzine de cibercultura Global Drome.



Portada de la web de FrEE

La razón de crear FrEE fueron los primeros intentos de Estados Unidos por censurar Internet, con la aprobación de la *Communications Decency Act* (Ley por la Decencia de las Comunicaciones):

> Somos un grupo de cibernautas españoles que queremos proteger la libertad de expresión en Internet. Por ello, tras haber contactado con varias organizaciones americanas que trabajan en este tema y contarnos su situación ante la CDA (Communications Decency Act), aprobada allí este año, hemos decidido que ha llegado el momento de empezar a actuar aquí también.[44]

FrEE se alió en sus inicios con la organización norteamericana de defensa de los ciberderechos Electronic Frontier Foundation aunque posteriormente se desvinculó, por divergencias ideológicas. Mantuvo también alianzas con la Global Internet Liberty Campaign (GILC), FITUG en Alemania, Cyber Rights & Cyber Liberties en Gran Bretaña, XS4ALL en Holanda, la Strano Network en Italia y la Asociación de Usuarios de Internet francesa.



Logo de FrEE

En su época de mayor auge, FrEE congregó a un equipo de 25 personas, que estaban en contacto a través de una lista de correo de organización interna. Entre ellos había destacados personajes de la vida internauta como **José Manuel Gómez**, autor del conocido boletín sobre criptografía “PGP Magazine” y la página PGP en español. En 1997 Gómez puso en marcha el proyecto Kriptópolis, que tuvo gran éxito. Con la ayuda entre otros del abogado Carlos Sánchez Almeida, también miembro de FrEE, *Kriptópolis* lideraría la importante lucha internauta contra la Ley de Servicios de la Sociedad de la Información, aprobada en 2002.

También estaban en FrEE el profesor Arturo Quirantes, los abogados Javier Maestre y el peruano Erick Iriarte, quien fundaría Alfa-Redi; el sindicalista y más tarde presidente de la Asociación de Internautas, Víctor Domingo, los periodistas Javier Villate, Ángel Cortés, José Antonio del Moral y Mercè Molist, y los ingenieros José Luís Martín Mas, Jesús Cea Avión y Óscar Reixa, quien aportaba el servidor en el que se alojaba la web.

> Oficialmente, no hay “hackers” entre nosotros, aunque estamos en contacto con ellos e intentamos dar un golpe de mano.[45]

3.1. Las huelgas pro Tarifa Plana

Las huelgas por la Tarifa Plana fueron la primera movilización masiva de la comunidad internauta española, que se alzó contra un aumento espectacular de tarifas por parte del entonces monopolio Compañía Telefónica Nacional de España. Al grito de **¡Tarifa Plana, Ya!**, se desató una gran protesta contra la que llamaban, ridiculizándola, **Timofónica**.



FrEE apoyó públicamente las huelgas y, sin ser el grupo más combativo, formó

parte de la organización de la tercera y cuarta. Su rol fue más cercano al consejo de sabios que a la horda guerrillera, siendo su principal tarea la distribución de textos que explicaban a los observadores qué estaba pasando y cómo interpretar aquel bullicio.

3.1.1. La primera huelga



Todo empezó, explica Joshua Llorach en Bandaancha, por el alto precio de las conexiones telefónicas, queja habitual de los internautas en los 90. Infovía, que apareció en 1995, había ayudado a rebajar mucho las facturas, ya que con una llamada local se podía acceder a Internet desde cualquier punto de la geografía española. Pero aún así seguía siendo caro y los internautas reclamaban una tarifa plana:

> Para acceder a Internet era necesario contratar los servicios de un proveedor. (…) Su coste rondaba las 12 mil pesetas anuales. Pero para llegar desde tu casa al ISP necesitabas usar la red telefónica. El 055 de Infovía tenia coste de llamada local y su precio era de 1,9 pesetas el minuto. Una hora conectado suponía 114 pesetas.[46]

Esta situación provocó la primera huelga, el 26 de enero de 1997, convocada desde la Lista de correo [tarifa_plana]. La movilización fue pequeña, más bien un ensayo de las que vendrían. Consistió en una *"huelga de teléfonos caídos"*: no usar el teléfono ni Internet y desconectar los contestadores.[47]



Portada de la web de Alberto Ruiz. Muchas páginas tenían este aspecto, repletas de "banners" y "gifs" reivindicativos

De la lista [tarifa_plana], que llegaría a tener la friolera de 3.000 suscriptores, salieron la *Plataforma Tarifa Plana*, liderada por **Luca Olivetti** y **José Ramón Esteban**, y la web Tarifaplana.vesatec.com, que puso en marcha **José Herreros** el 5 de julio de 1996. Otros punteros de la lucha fueron las páginas informativas que creó Luca Olivetti, hoy desaparecidas, y http://www.telecom.eu.org/es/index.htm de José Ramón Esteban[48], quien a finales de 1997 auspició también el grupo de noticias es.charla.conexion.tarifa-plana. Había además multitud de páginas personales que se pusieron al servicio de las movilizaciones, ofreciendo información y *banners* reivindicativos, como la de Alberto Ruiz Rodrigo creada el 12 de febrero de 1997.





Era recurrente en esos *banners* usar el logotipo de la compañía Telefónica, reconvertida en Timofónica, por lo que Telefónica hizo una denuncia masiva a decenas de páginas, entre ellas Timofonica.com, obra de los autores de Isla

Tortuga, **Angeloso** y **Maki**. Los jueces sobreseyeron todas las denuncias.[49]

3.1.2. El aumento de tarifas inflama la red: segunda huelga

La situación se complicó cuando, a mediados de 1997, se supo que Telefónica aumentaría tarifas[50]. La subida en las llamadas locales sería del 137% y la hora de acceso a Internet pasaba de costar 114 pesetas a 270.



La indignación bullía en los foros de la red. La protesta contra Telefónica se convirtió en tema número uno de las conversaciones, donde se proponían recogidas de firmas, envío de cartas a la Comisión del Mercado de las Telecomunicaciones y otras acciones. Ejemplo de ello son los mensajes registrados en es.charla.conexion.tarifa-plana: en enero de 1998 se mandaron 111 mensajes al grupo. En septiembre del mismo año, en el epicentro de la segunda huelga, fueron 2.626 mensajes, cifra que se mantuvo estable, con picos de hasta 4.000 mensajes, entre 1999 y 2000.

Cuando Telefónica empezó a aplicar la subida de precios, en abril de 1998, la comunidad internauta se levantó de forma unánime. El punto central de información era la web *www.lanzadera.com/lahuelga*, de donde surgiría la *Plataforma La Huelga*, después Plataforma Internauta, cuyos líderes eran **Yonko**, **Fonco** y **Pilar Gías**.



Plataforma Tarifa Plana, *Plataforma La Huelga* y el *Grupo Tarifa Plana* de **Imanol Alberti** y **Juanga Covas** convocaron una huelga para el 3 de septiembre de 1998. Pedían la implantación de una tarifa plana de conexión a Internet y la ampliación del horario de tarifa reducida, que en la mayoría de países europeos empezaba a las 18.00 hasta las 08.00, mientras que en España empezaba a las 22.00.[51]



Contaron con el apoyo unánime de todo tipo de grupos de internautas, más o menos organizados, que habían surgido de los chats, listas y grupos de noticias. FrEE estaba entre ellos, así como la Asociación de Usuarios de Internet (AUI), que intentaría ponerse al frente de las reivindicaciones con el argumento de que había recogido 12.000 firmas por la tarifa plana.

La AUI era una organización surgida en 1995 bajo los auspicios y el billetero de compañías como Microsoft, que querían tener un Caballo de Troya en la comunidad internauta. Su principal actividad era montar un congreso para empresas, Mundo Internet, en Madrid. Aunque en un principio despistó a los grupos convocantes, quienes le dieron crédito, pronto se vería que trabajaba en beneficio de Telefónica.

3.1.3. De la AUI a la AI

A falta de datos, la huelga fue sentida como un éxito por la comunidad internauta. La AUI propuso una reunión de los grupos convocantes y simpatizantes, para *"iniciar un diálogo conducente a un acuerdo satisfactorio para todos"*[52], como se explicaba en un nuevo comunicado de FrEE. Pero esta reunión acabó siendo una encerrona de Telefónica, con la complicidad de la AUI, que pretendía ofrecer unos planes de descuento para acabar con la reivindicación.

Esta página secunda la huelga de usuarios de Internet en demanda de unas tarifas justas.

Disculpen las molestias que les podamos estar causando. Mañana este sitio mostrará su aspecto habitual. Gracias.



Quienes tenían páginas web seguían la huelga "cerrando" la web, es decir, ofreciendo ese día una portada especial y sin permitir el acceso al resto de contenidos. Concretamente, así se veía el famoso sitio Dios Proveerá en las huelgas de septiembre y octubre

La propuesta de Telefónica indignó a la comunidad y se convocó un nueva huelga, el 3 de octubre de 1998. Esta vez FrEE sería también convocante, junto con el *Grupo Tarifa Plana* (GTP), la *Plataforma La Huelga* (PLH), y la *Plataforma Tarifa Plana* (PTP), que formaron la *Coordinadora pro Tarifa Plana*. El diario "El Mundo" entrevistó a diversos representantes de la lucha internauta, entre ellos a David Casacuberta, quien criticó públicamente a la AUI,

> El hecho de que los internautas busquen nuevas formas de asociación tiene que ver con el papel que ha jugado la AUI en nuestro país. Tenemos la sensación de que esta asociación no representa a los usuarios de la Red y su labor ha estado más cercana al ámbito empresarial que al social. [53]

La Coordinadora emitió también un comunicado en el que deslegitimaba a la AUI, por tener intereses comerciales con Telefónica.[54]

En los días previos a la huelga, la Coordinadora se comunicaba en un canal de chat privado. FrEE designó a tres representantes para las conversaciones: Javier Villate, Mercè Molist y Víctor Domingo. Este último[55] fue el que más se implicó en la idea de dar continuidad a la Coordinadora más allá de la huelga, creando una asociación que cogiese el testigo de la reivindicación y fuese un interlocutor válido de los internautas frente al gobierno.



Víctor Domingo, en el centro, y Juan Gabriel Covas (SonnY) a su izquierda, miembros de la junta de la recién creada Asociación de Internautas, con el equipo que saltó el Viaducto de Segovia para colgar en él dos pancartas pro Tarifa Plana[56]

Así, una semana después de la tercera huelga, el 10 de octubre de 1998, en una reunión en Madrid se fundó la Asociación de Internautas. En su junta directiva había representantes de FrEE, *Grupo Tarifa Plana*, *Plataforma Internauta* y *Plataforma Tarifa Plana*.[57][58]

Esta huelga fue la primera en la que se manejaron cifras, aunque fueron de chiste: según Telefónica la siguieron el 7% de sus clientes, frente al 70% según los convocantes.[59]

3.1.4. Cómo se desactivó la protesta



La Asociación de Internautas llevó a cabo diversas acciones más allá de la red, como colgar pancartas en Madrid o llenar la feria SIMO de folletos reivindicativos.

La comunidad celebró con gran ilusión el nacimiento de la *Asociación de Internautas* (AI), pero la realidad frustró los ánimos. Las conversaciones con el Ministerio de Fomento se convirtieron en un tira y afloja, más parecido a

maniobras dilatorias del gobierno para capear el temporal que a un auténtico intento de arreglar las cosas. La misma actitud mostró Telefónica, quien ofreció un sistema de bonos como remedo de la tarifa plana, que pronto fueron llamados *timobonos*.

El Senado también se metió, a través de su Comisión de Internet, que a pesar de generar mucho ruido en la prensa nunca consiguió llevar la reivindicación a buen término, sólo generó más dilaciones, conversaciones infructuosas y papel mojado que acabaron cansando a la comunidad internauta. Además, aparecieron personajes como Mikel Amigot, director de *LaBrujula.net*, ansiosos de tocar poder gracias a la lucha internauta, que en vez de ayudar añadieron más leña al fuego.[60]

No fueron esos los únicos oportunistas que se arrimaron a la tarifa plana. Los proveedores de acceso a la red vieron una oportunidad comercial en tan ferviente demanda popular y no pasó mucho tiempo sin que anunciasen sus ofertas de "tarifa plana" que no eran tales: por una tarifa fija de alrededor de 3.000 pesetas daban acceso a Internet pero, como explicaba Bandaancha, *"sólo podías conectarte a partir de las 18h y durante fines de semana y festivos si no querías llevarte una sorpresa con la factura"*[61]. La comunidad internauta lo llamó **tarifa ondulada**.

Hubo dos huelgas más, el 31 de enero de 1999[62][63] y el 6 de junio del mismo año[64], que ampliaron su radio de acción a toda Europa, con la participación de organizaciones de Austria, Bélgica, España, Francia, Gran Bretaña, Grecia, Italia, Polonia, Portugal, República Checa, Rumanía, Suecia, Holanda, Grecia y Suiza, además de la Asociación de Usuarios de Internet argentina. La reivindicación era para todos la misma: protestar contra la subida de las tarifas telefónicas.

El 10 de agosto del 2000, FrEE anunciaba su disolución y abandonaba la lucha por la tarifa plana, que quedaba totalmente en manos de la Asociación de Internautas.

4. El Hackmeeting

Un hackmeeting es un congreso de hacktivistas. Como otras reuniones de hackers consiste en unos días de encuentro donde se realizan charlas, talleres y otras actividades. Su elemento diferenciador es que al contenido técnico se une la reivindicación social.



Sala de ordenadores del hackmeeting celebrado en Madrid en 2002, el más multitudinario de los hackmeetings celebrados en el estado español

4.1. Historia

La idea y también *franquicia* (en cierto sentido) de los hackmeetings nació en Italia. El primero se celebró en Florencia, en junio de 1998[65] y duró 3 días. Lo organizaron la asociación Strano Network, que formaba parte del proyecto net-activista Isole Nella Rete, y el Centro Popolare Autogestito (CPA) di Firenze Sud, una antigua fábrica okupada donde tuvo lugar el encuentro. La ubicación no era una casualidad: los hackmeetings se celebran siempre que es posible en sitios okupados o centros sociales y su organización es asamblearia.

> El encuentro simbolizaba, por primera vez en el universo de las “hacker con’s”, la unión de la comunidad alternativa (también llamada “antagonista”) con los magos y dioses de Internet. Unión patente no sólo entre los asistentes (unas 200 personas) sinó también entre los casi 300 individuales y grupos que mostraron su solidaridad con el evento: desde los canales #cyberpunk y #komunisti de Undernet, hasta la Casa Okupada de Mujeres La Eskalera Karakola de Madrid.[66]

El proyecto *Isole Nella Rete* era muy conocido en el panorama cíberactivista de Europa, con multitud de contactos y lazos que se hicieron patentes en el encuentro: junto a otros colectivos hacktivistas italianos como Tactical Media Crew

o la revista ciberpunk *“Decoder”*, asistieron los holandeses *XS4ALL* y Hippies from Hell, la BBS de artistas europeos y norteamericanos The Thing y los españoles de Nodo50, capitaneados por **Alberto Escudero**, quienes ayudaron en la organización.[67]

Se decidió que los hackmeetings tendrían periodicidad anual y sede itinerante, así que el siguiente fue en Milán[68]. Allí acudió otra vez Nodo50 y también Sindominio, un nuevo ISP alternativo español surgido de una escisión de Nodo50.

En un aparte de aquel hackmeeting, una conversación entre **Roxu** y Adolflow, ambos de Sindominio, y la periodista y activista de FrEE **Mercè Molist**, derivó en la idea de hacer un evento parecido en la Península Ibérica. Al volver de Italia siguieron las conversaciones y todo se afianzó: Sindominio se encargaría de la infraestructura y Molist, en nombre de FrEE, coordinaría el equipo humano y el contenido.

La comunidad okupa catalana ofreció la casa Les Naus como sede del evento, en el barrio de Gracia de Barcelona, además de la ayuda de algunos de sus miembros. Diversos integrantes de Sindominio (**Miquel**, Roxu, **Joanma**, **Magda**, **Joseba**, **Patxangas**, **Alejo**, etc) ayudaron a distancia, a través de la lista de correo de coordinación, que funcionaba como asamblea. Pronto se les unieron hackers independientes como el desarrollador de una de las primeras redes P2P, Gnutella, **Esteve Fernández**, **_RaMoNe_**, **Elrojo**, **Àlex Castán**, **Peyote**, **Hubble**, **Toni Panadès** (artífice del IRC-Hispano), **Javier Martinez Martí**, **Ursus Furus**, **Flynn Kobe**, **N.B.K.** (de Alea Hackta Est), **Pancake** (de CatHack), **Chus forever**, **Deal**, **astrid77**, el periodista **Sergi Bueno** y más.[69]

Alberto Escudero y Mercè Molist viajaron al hackmeeting italiano, que aquel año 2000 se celebraba en Roma[70], y explicaron a la asamblea que se estaba organizando el primer hackmeeting del estado español, noticia que la comunidad italiana recibió con alegría. Una nutrida representación de la misma asistiría al encuentro de Barcelona y siguientes.

4.2. Barcelona, Leioa, Madrid, Iruña, Sevilla...

El primer hackmeeting del estado español se celebró los días 20, 21 y 22 de octubre del 2000 en Barcelona.



Según la prensa que cubrió el evento[71] asistieron unas 300 personas, que abarrotaron el edificio de Les Naus. Entre las charlas con más asistentes, el *Taller de cabinas*, que impartió **Green Legend**, de SET; *Introducción a la computación cuántica*, de **GekM**; *Echelon y la Gran Familia*, del miembro de FrEE **Arturo Quirantes**; *Programas autorreplicantes*, de **Wintermute** (29A), o el debate *Tarifa Plana y futuro de la lucha internauta*, coordinado por **Roberto Pili**.

El resto de charlas, talleres y debates[72] contaron con oradores como el experto en arte electrónico José Luis de Vicente; el creador de la pionera red ciudadana TINET **Manuel Sanromà**; los diseñadores **Antaviana**; **Zhodiac** de !Hispahack; el presidente de FrEE David Casacuberta; los hackers **Manu**, **Marc**, **Endika**, **Ibai**, Hubble, José Luis Martín Mas, **Jaime Agudo**, **Oscar Conesa**; el apòstol de FreeBSD **Jesús Rodríguez**; los *artivistas* Fiambrera Obrera y el equipo **esCERT** de respuesta a incidentes informáticos.

Siguiendo la tradición italiana, el último acto del hackmeeting fue la fundación del hacklab de Barcelona Kernel Panic, que tuvo su sede en el centro okupado La Akademia hasta que fue desalojado un año después. Posteriormente y con los ordenadores *parriba*, *pabajo* estuvo en diversos sitios okupados y después desalojados, incluído Les Naus, donde permaneció más tiempo (dos años, hasta 2003).



Programa de charlas del hackmeeting de Madrid

El hackmeeting de Barcelona se consideró un éxito[73] y fue la semilla para la celebración de otros, cada año y de forma itinerante. El más multitudinario fue el de Madrid, celebrado en 2002, al que asistieron unas 600 personas[74], entre ellas italianos, mexicanos y norteamericanos.

El capítulo español de Computer Professionals for Social Responsability, básicamente la misma gente que había estado en Fronteras Electrónicas, finiquitada en el 2000, presentó en el hackmeeting de Madrid y por primera vez en el estado español la entrega de los Premios Big Brother[75][76]. Diversos grupos de ciberderechos organizaban estos premios en eventos de todo el mundo, para llamar la atención sobre empresas y gobiernos que atentaban contra la privacidad electrónica. La ceremonia, organizada y presentada por Arturo Quirantes, se repitió en los hackmeetings de Iruña[77] y Sevilla[78].



Barcelona. 2000. CSOA les Naus

Leioa. 2001. Gaztetxe de Udondo - Bilbao[79][80][81][82]

Madrid. 2002. Labo03, Lavapiés

Iruña. 2003[83][84][85]

Sevilla. 2004. La casa de la paz[86][87]

Menorca. 2005. Es Mercadal

Mataró. 2006. CSOA La Fibra

Gernika. 2007. CSOA Astra Gernikeko Gaztetxea

Málaga. 2008. La casa invisible

Madrid. 2009. Patio Maravillas[88]

Zaragoza. 2010. Antigua cárcel de Torrero

A Coruña. 2011. CSOA Palavea.

Vallbona d'Anoia. 2012. Calafou.

4.3. Ataques y críticas

Diversos grupos de hackers asistieron, dieron charlas y ayudaron a organizar los primeros hackmeetings, dejando constancia de ello en sus ezines: SET[89][90], 7a69ezine[91], Undersec, NetSearch[92], Proyecto_R[93]. Pero el evento también cosechó críticas, normalmente por la mezcla de lo político con lo técnico, que tanto en Italia[94] como España[95][96][97] no gustó a toda la comunidad hacker.

> Nosotros nos pasamos por la hackmeeting (Buen ambiente, buen rollo, demasiada politica)[98]

Pero la mayor polémica se vivió en la segunda edición del hackmeeting español, en Leioa (Bilbao), debido a unas fotos de la casa donde se celebraba el hackmeeting, en el que algunos vieron pintadas pro-terrorismo. La noticia salió en diversos medios[99] y un grupo desconocido, **Mat Team**, *defaceó* la web del hackmeeting, hazaña que dedicó a *"las víctimas del terrorismo etarra"*[100]. Más tarde se supo que Mat Team era un chaval de Vallecas.

Vinieron después cuatro años de calma hasta que, en enero de 2005 y por ninguna razón concreta, el servidor de Sindominio sufría un nuevo ataque, con *deface* incluído de la web del hackmeeting[101]. Los intrusos firmaron como pr0j3kt m4yh3m y dejaron el siguiente mensaje:

> "estamos hasta la polla de gente como vosotros que por saber lo que es un modem se creen hackers, y que ademas lo utilizan para vender su mierda de politica"
>
> (...)
>
> Sindominio.net / hacklabs.org / indymedia / nodo50.org: Mezclan hack con política (ultra izquierda) que cojones tiene que ver el código libre con okupar casas?.

Además de la relación de algunos de sus miembros con la izquiera abertxale (ETA).**[102]**

4.4. CatHack

CatHack! fue uno de los grupos hacker que más apoyó al Hackmeeting y también estuvo vinculado con el Hacklab de Barcelona. A diferencia del resto de la escena, CatHack! afirmaba ser sensible a lo político-social[103]:

> Todos estamos en mayor o menor medida politizados al contrario que muchos otros grupos, quiza esto nos es un gran punto de critica por mucha gente de la 'scene', que prefieren no mezclar los conceptos hack + activismo.[104]



Nació a finales de 1998 en Barcelona y murió en 2005. Lo formaban **Barner**, **Pop**, **Asef** y **PGB**. Parece que más tarde se les unió **Kuduk**. CatHack tenía una web, hoy desaparecida; un canal en el IRC-Hispano, #cathack, y una lista de correo. El grupo publicó 9 números de su ezine, cuyo editor fue Pop (también conocido como *pancake*). Es la única ezine hacker en catalán.

> La idea principal era la de poder intercambiar informacion y conocimiento sobre tematica hpcva (hack/phreak/crack/virii/activism) en la lengua con la que nos hemos criado y mejor nos sabemos expresar.[105]

5. Los hacklabs

Un hacklab[106] es un *laboratorio hacker*. Se parece más a un grupo de usuarios de software libre que a un grupo hacker. Tiene una sede en el Mundo Real, muchas veces en un centro social u okupado, donde sus integrantes se reúnen de forma periódica para charlar, aprender, montar proyectos, hacer cursos... y una lista de correo para el contacto más diario. Las principales preocupaciones de un hacklab son la libertad de la información y del software y el control que los poderosos ejercen mediante la tecnología.[107]



Las acciones que suele realizar un hacklab son:

> Dar uso a viejos ordenadores. Construir redes de todo tipo. Experimentar con cortafuegos, con redes inalámbricas, con usos útiles y también con usos inútiles de las máquinas. Hacer charlas y seminarios, talleres y demostraciones públicas que permitan acercar a la gente tecnologías que se quieren presentar como solo aptas para expertos (...). Sacar a la luz y organizar la resistencia contra todo aquello que trata de obstaculizar la libertad en todas sus formas, en la red y fuera de ella. En fin, construir instrumentos de comunicación y redes libres para una sociedad libre.[108]

Actualmente, (2013), los hacklabs viven un buen momento en Latinoamérica (más arriba puede verse el logo del HackLab Autónomo, en México), mientras languidecen en Europa.

5.1. Historia

Las primeras reuniones periódicas de hackers en un sitio físico surgieron en Estados Unidos, entre 1975 y 1986, en el famoso Homebrew Computer Club de la segunda generación de hackers. El objetivo de sus fundadores era poner en contacto a genios del hardware para que creasen ordenadores accesibles para todo el mundo. Entre sus asiduos, los jóvenes Steve Wozniak (Apple Computer), Harry Garland y Roger Melen (Cromemco), George Morrow (Morrow Designs), Adam Osborne (Osborne Computer) y Bob Marsh (Processor Technology).

La tercera generación de hackers trajo consigo otras reuniones, como los

encuentros mensuales en puntos de todo el planeta, organizados por forofos de la revista norteamericana 2600: The Hacker Quarterly, que nació en 1984.

En Europa, el grupo alemán Chaos Computer Club montaba encuentros periódicos en los 90, pero en el sur no hay nada hasta que aparecen los hacklabs en Italia, como sitios físicos de intersección entre la tecnología y la acción social. El primero fue el Freaknet Medialab, que nació en 1994 como BBS y se estableció como hacklab en el *Centro Sociale Auro*, en Catania (Sicilia), en 1997.

El fuelle de los hacklabs fueron los hackmeetings, al establecerse la tradición de crear un nuevo hacklab allí donde se acababa de celebrar un hackmeeting, para aprovechar las sinergias generadas por el mismo. El primer hacklab hijo de un hackmeeting fue el de Florencia, en 1998.

Cuando empezaron a hacerse hackmeetings en España, con ellos llegó la tradición de los hacklabs. El primero, Kernel Panic, se creó tras el hackmeeting de Barcelona, en el año 2000.

Después vinieron el Metabolik BioHacklab (2001) en Leioa y el Cielito Lindo (2002), después rebautizado **Wau Holland 2001**, en Madrid. El éxito fue tal que pronto aparecieron hacklabs, como los de Zaragoza, La casa encantada en Santiago de Compostela o el muy activo VallekasLab, sin necesidad de haberse celebrado previamente un hackmeeting.

Se creó una lista de correo de coordinación, la Hacklabs Mailing List y un sitio web donde estaba centralizada la información de todos los hacklabs no sólo españoles sino del mundo.



Detalle de la Jornada Interhacklabs

El punto culminante de este movimiento lo marcaron las **Jornadas Interhacklabs**, que organizó el activo Hacklab de Vallecas en Madrid, en abril de 2006. Acudieron medio centenar de personas, representando a los 22 hacklabs que en aquel

momento había en España[109].

Las Jornadas Interhacklabs marcan el inicio de la decadencia del fenómeno, que muere oficialmente en 2009, cuando su principal símbolo, el hacklab de Barcelona, tira la toalla después de una larga agonía y el cierre de la mayoría de hacklabs de referencia.

5.2. Qué hicieron los hacklabs

Una de las campañas más exitosas de los hacklabs en España fue **Compartir es bueno**.



Consistió en acciones en sitios públicos, donde se repartían CDs con música libre o se descargaban canciones con *copyright* de las redes P2P, como provocación y crítica a las entidades gestoras de derechos de autor. *Compartir es bueno* surgía del imperativo de liberar la información que dicta la ética hacker, algo que los hacklabs se toman muy en serio, usando sólo programas libres y publicando todos sus contenidos bajo licencias libres.



Otra original idea fueron las fiestas **Hacking The Streets**: consistían en sacar mesas y ordenadores del hacklab a la calle y mostrar la tecnología a los vecinos, amén de regalarles programas libres e incluso instalarlos en sus ordenadores, al más puro estilo *install party*.[110]



El Metabolik BioHacklab creó la LiveCD X-Evian[111], una distribución autoinstalable con programas pensados para las y los activistas, como cifrado, edición de video, retoque de fotos y un navegador con enlaces a páginas activistas.[112]

Los hacklabs estaban muy comprometidos con la transmisión del conocimiento y el aprendizaje, por lo que organizaron multitud de cursos[113], jornadas y charlas, como las jornadas **Jocs Fractals** en Barcelona, en 2003[114][115] y 2005[116][117][118], y las **Jornadas Telemáticas** de Vallecas, de 2003 a 2006.[119]

5.3. Madres y padres del hacktivismo

El fenómeno hacklabs en el estado español funcionaba como un reino de taifas, donde cada hacklab trabajaba de forma autónoma y, si era necesario actuar unidos, los contactos se realizaban más entre individuos que oficialmente entre los grupos. Así nació el hacktivismo más militante, más guerrillero, que simbolizan los hacklabs: sin puntos centrales de control, con múltiples células autónomas capaces de conectarse y desconectarse a la velocidad del rayo.



Performance del Hacklab de Barcelona, disfrazados como terroristas de la distribución de GNU/Linux Debian

Así, podríamos decir que de Fronteras Electrónicas nació el *hacktivismo blanco*, de salón, donde se luchaba ofreciendo información y opinión. Y de los hacklabs nació el *hacktivismo gris*, de acción, padre directo de fenómenos como **Anonymous** y más allá. No debe extrañar que, a la decadencia de la lista de correo de los hacklabs, la siguiese la creación de la lista de correo Hacktivistas: parte de sus habituales son viejos veteranos del movimiento de los hacklabs, que dio experiencia y cuerpo teórico a todo el hacktivismo posterior.

6. Notas

1. ↑ Declaración de Independencia del Ciberespacio. John Perry Barlow. Trad. de Biblioweb
2. ↑ Quién es Richard Stallman. modernclics. Preguntas Linux (13-07-05)
3. ↑ GNU. Es.Wikipedia
4. ↑ Código hispano. Mercè Molist para "Ciberpaís" (08-99)
5. ↑ Un estudio denuncia la 'hostilidad' contra la mujer en los entornos tecnológicos. Mercè Molist para "Ciberpaís" (06-07-06)
6. ↑ @javiespejo (15-07-13)
7. ↑ BULMA: Asociación de Bisoños Usuarios de Linux de Mallorca y Alrededores. Maribel García. "Ciutat de Mallorca" (29-03-01)
8. ↑ (Comandob) BULMA at Hackstory. Javi Polo. Lista de correo Comandob (13-02-13)
9. ↑ Berto, en conversación privada
10. ↑ Ricardo Galli, en conversación privada
11. ↑ (Comandob) BULMA at Hackstory. Javi Polo. Lista de correo Comandob (13-02-13)
12. ↑ Respuesta de Benjamí Villoslada. Twitter (14-02-13)
13. ↑ Ricardo Galli, en conversación privada
14. ↑ Balearikus Party el 12 de Mayo del 2000. Gabriel. Weblog BULMA (11-05-00)
15. ↑ Ya llega la Balearikus Party II. Gabriel. Weblog BULMA (17-10-2001)
16. ↑ Conferencias en Balearikus Party. René Mérou. Weblog BULMA (04-12-2001)
17. ↑ Historia. Javier Cantero. Web de es.comp.os.linux (25-06-02)
18. ↑ Pingüinos al poder. Mercè Molist para "Ciberpaís". 1998
19. ↑ Historia. Javier Cantero. Web de es.comp.os.linux (25-06-02)
20. ↑ Humor. Web de es.comp.os.linux.*
21. ↑ Hacker. The Jargon File, version 4.4.8 "The New Hacker's Dictionary". Eric S. Raymond
22. ↑ RESULTADO: es.comp.os.linux pasa 68:0. Jose Miguel Femenia Herrero (23-08-96)
23. ↑ RESULTADO: es.comp.os.linux.anuncios pasa 67:0. Jose M. Femenia Herrero. CORUS-ES: moderacion de es.* (07-02-02)
24. ↑ Bilo y Nano cumplen 3 años de humor informático. Mercè Molist para "Ciberpaís" (02-02-04)
25. ↑ Bilo y Nano cumplen 3 años de humor informático. Mercè Molist para "Ciberpaís" (02-02-04)
26. ↑ Hacktivismo FAQ. Cult of the Dead Cow
27. ↑ Entrevista Ricardo Domínguez
28. ↑ The Zapatista Tactical FloodNet. EDT
29. ↑ Ricardo Domínguez: "Es mejor que tumben un servidor a que te den un balazo". Mercè Molist para "Ciberpais" (13-11-02)
30. ↑ El Pentágono, contra el recién nacido "hacktivismo". Mercè Molist para "Ciberpaís" (1998)
31. ↑ The Portuguese Scene. Eurinomo y Quickzero. Phrack Magazine #65 (11-04-08)
32. ↑ HACKED Timor. 2600 Who have they Hacked Now (22-11-97)
33. ↑ Campaña Timor Oriental. Toxyn
34. ↑ KEPOLISIAN REPUBLIK INDONESIA - HOMEPAGE - Indonesian National Police. Sitio hackeado el 19-01-98
35. ↑ KEPOLISIAN REPUBLIK INDONESIA - HOMEPAGE - Indonesian National Police. Sitio hackeado el 19-01-98
36. ↑ Entrevista Jordi Murgó. Revista @rroba, 95 (04-05)
37. ↑ The VERY popular imapd remote overflow. Insecure.org
38. ↑ Introduction to QueSO. By savage@apostols.org
39. ↑ Remote OS detection via TCP/IP Stack FingerPrinting. Fyodor (18-10-98)
40. ↑ Un programa catalán causa el pánico en Israel. Mercè Molist (1998)
41. ↑ La inconfesable historia del Nodo50 . "De Sur a Sur. Revista andaluza de solidaridad, paz y cooperación". N. 14 (03/98)
42. ↑ La inconfesable historia del Nodo50 . "De Sur a Sur. Revista andaluza de solidaridad, paz y cooperación". N. 14 (03/98)

43. ↑ La inconfesable historia del Nodo50 . “De Sur a Sur. Revista andaluza de solidaridad, paz y cooperación”. N. 14 (03/98)
44. ↑ Sobre Nosotros. Web de Fronteras Electrónicas de España (10-10-97)
45. ↑ Viviendo en la frontera. *Mercè Molist para “Ciberpaís” (1996)*
46. ↑ Aquel verano del 98. Josh. Bandaancha.eu (11-10-08)
47. ↑ Quiénes somos. Asociación de Internautas
48. ↑ Octubre. Aniversarios, defunciones y enfermos terminales. En mi humilde opinión (25-10-09)
49. ↑ CASO VESATEC vs. TIMOFONICA. Timofonicas.com (11-98)
50. ↑ Telefónica y el Gobierno han decidido subir el precio de las llamadas metropolitanas. Alberto Ruiz Rodrigo
51. ↑ FrEE exige tarifa plana y ampliación del horario de tarifa reducida. Comunicado 31/08/98
52. ↑ Comunicado de FrEE tras el 3S (8-9-98)
53. ↑ Entrevista con David Casacuberta (Presidente de Fronteras Electrónicas España). El Mundo, 20/09/98
54. ↑ COMUNICADO CONJUNTO DE FrEE, GTP , PLATAFORMA LA_HUELGA Y PTP Y GRUPO MOVILIZACIÓN (17-09-98)
55. ↑ Víctor Domingo: Presidente, presidente. Mercè Molist para “@rroba” (29-05-07)
56. ↑ La Tarifa Plana se descuelga en el Viaducto de Segovia en Madrid. Asociación de Internautas (08-06-00)
57. ↑ Acta fundacional. Asociación de Internautas (10-10-98)
58. ↑ Quiénes somos. Asociación de Internautas
59. ↑ Los internautas quieren que Aznar avale la tarifa plana de acceso a la red. “El País” (06-10-98)
60. ↑ El Senado desaprueba la actuación de Telefónica sobre el mapa tarifario. Computerworld (30-10-98)
61. ↑ Aquel verano del 98. Josh. Bandaancha.eu (11-10-08)
62. ↑ Europa, en Huelga por la Tarifa Plana. Alberto de las Fuentes. “El Mundo” (31-01-00)
63. ↑ FrEE llama a la huelga el día 31. Comunicado 28/01/99
64. ↑ La huelga del 6 de junio de 1999. Movilizaciones por la tarifa plana. Dios Proveerá
65. ↑ HackIt’98
66. ↑ Europa organiza la autodefensa digital. “Ciberpaís“ (06/98)
67. ↑ Breve historia del Hackmeeting (2004). Adolfo Antón Bravo (20/12/04)
68. ↑ Hackmeeting99
69. ↑ Lista hackmeeting Barcelona (02/01)
70. ↑ Hackmeeting 2000
71. ↑ Los hackers hacen su primer congreso en una casa «okupada». “El Mundo” (23/10/00)
72. ↑ Programa Hackmeeting BCN’00
73. ↑ Ya llega el Hackmeeting Leioa 2001. Barrapunto (21/09/01)
74. ↑ Internautas reunidos en Madrid piden la retirada de la LSSI. Mercè Molist (06/10/02)
75. ↑ Premiados en la primera edición de los BBA-Spain. Libertad Digital(10-05-03)
76. ↑ [nettime-lat *CPSR-ES CONVOCA LOS PREMIOS BIG BROTHER ESPAÑA]*. Nettime mailing list archives (11-09-02)
77. ↑ Big Brothers Awards. Bitácora de Markoss. Barrapunto (01-10-03
78. ↑ Los músicos se unen al Hackmeeting con un concierto libre. Mercè Molist para “Ciberpaís” (30-10-04)
79. ↑ El Hackmeeting 2001 arrasa. Entorno de ACS (24/09/01)
80. ↑ Un diario vincula con el “entorno etarra” a la organización del congreso de hackers de Leioa. Cybereuskadi (04/09/01)
81. ↑ ‘Piratas’ en el ‘gaztetxe’. “El País” (23/09/01)
82. ↑ Los “piratas” defienden la paz. “El Mundo” (27/09/01)
83. ↑ Los ‘hacker’ no son tan malos. “El Mundo” (26/10/03)
84. ↑ Hackmeeting 2003 de Pamplona debate el canon y los derechos de autor. “Ciberpaís” (30/10/03)

85. ↑ Mujeres y extranjeros se unen al hackmeeting. Mercè Molist (26/10/03)
86. ↑ Blog del Hackandalus
87. ↑ Los músicos se unen al hackmeeting. Mercè Molist (30/10/04)
88. ↑ Los hackers salen al patio. Miguel Criado. "Público" (11/10/09)
89. ↑ Under Updates. Opina, Critica, Comenta… gnd. SET-24 (05/02/01)
90. ↑ Hackmeeting 2002 / Madhack'02. Bazar. SET-26 (30/10/02)
91. ↑ Un 'finde' en la hackmeeting. Ripe. 7a69ezine#10
92. ↑ En contacto con Wintermute. NetSearch E-Zine 6 (02/07/2001)
93. ↑ Cronica del hmBCN '2000. TnK. Proyecto_R número 10 (12/00)
94. ↑ HackIt06: + Política -Técnica
95. ↑ ¿Que pasa con el hackmeeting? POR ALUSIONES. *Lista de correo de coordinación del Hackmeeting (03/01)*
96. ↑ Charlando con… CatHack!. 7a69ezine#14 (21/10/2002)
97. ↑ CatHack! 6
98. ↑ Presentacion. 7a69ezine#10
99. ↑ Un diario vincula con el "entorno etarra" a la organización del congreso de hackers de Leioa. Cybereuskadi (04/09/01)
100. ↑ Boicotean 'sindominio.net' para protestar contra el Hackmeeting que se celebra en Leioa a finales de mes. *"El Mundo" (10/09/01)*
101. ↑ Archivo de dSR. (16/08/05)
102. ↑ Crackeado Sindominio. Indymedia Euskal Herria (26/01/05)
103. ↑ Charlando con… CatHack!. 7a69#14 (21-10-2002)
104. ↑ Charlando con… CatHack!. 7a69#14 (21-10-2002)
105. ↑ Charlando con… CatHack!. 7a69#14 (21-10-2002)
106. ↑ Hacklab. Es.Wikipedia
107. ↑ ¿Qué es un hacklab?. Preguntas Frecuentes. Hacklabs
108. ↑ ¿Qué es un hacklab?. Preguntas Frecuentes. Hacklabs
109. ↑ El buen momento de los hacklabs favorece el activismo digital dentro y fuera de la red. Mercè Molist para "Ciberpaís" (04-04-06)
110. ↑ Hacklabs. Tecnologías y redes de ensamblado colectivo de autonomía digital v.0.9. *Xabier Barandiaran (16-12-03)*
111. ↑ X-Evian. Es.Wikipedia
112. ↑ Hacklabs. Tecnologías y redes de ensamblado colectivo de autonomía digital v.0.9. *Xabier Barandiaran (16-12-03)*
113. ↑ Cursos llevados a cabo en el Hacklab Kernel Panic
114. ↑ Jocs Fractals de la Vila de Gràcia. Quim Gil. Llista correu Debian en català (05-09-03)
115. ↑ PART DE LA "INTELLIGENTZIA" CIBERNÈTICA ES REUNEIX ALS PRIMERS JOCS FRACTALS. Mercè Molist (21-09-03)
116. ↑ II Jocs Fractals. Simó Albert. Hacklabs Mailist (23-02-05)
117. ↑ L'Hospitalet, seu dels segons Jocs Fractals. Vilaweb (11-03-05)
118. ↑ Programa dels II Jocs Fractals. Kernel Panic (15-03-05)
119. ↑ Programa Segundas Jornadas Telemáticas. KasLab (29-06-04)

7. Enlaces externos

7.1. La comunidad libre

· grupo de noticias es.comp.os.linux
· es.comp.os.linux.instalacion
· es.comp.os.linux.misc
· es.comp.os.linux.redes
· es.comp.os.linux.programacion
· es.comp.os.linux.anuncios
· Web de es.comp.os.linux.*
· Linux-es
· GULUC3M. Grupo de Usuarios de Linux de la Universidad Carlos III de Madrid.
· Astur Linux
· La imparable historia del “software” y la cultura libres. Mercè Molist para “Ciberpaís” (11-02-08)

7.2. La comunidad hacktivista

· Nodo50
· ¿Por qué Nodo50 se ha mudado a Suecia?. (29-07-11)
· Conversación con Ricardo Domínguez. Mercè Molist (13-11-02)

7.3. T0XyN

· East Timor. Archivo páginas hackeadas de la revista 2600.
· The Portuguese Scene. Eurinomo y Quickzero. Phrack Magazine #65 (11-04-08)

7.4. FrEE y las huelgas por la tarifa plana

· Comunicados de Fronteras Electrónicas
· Privacidad en Internet. Documento sobre la importancia que tiene la preservación de la privacidad en Internet, y descripción de las distintas técnicas que existen para protegerla, por José Luis Martín Mas. Presentado en la comparecencia de David Casacuberta, presidente de FrEE, ante la Comisión Especial del Senado sobre Internet, 16 de junio de 1998.
· Los internautas se preparan para una nueva protesta. El Mundo, 17/09/98.
· De vuelta a las trincheras. “El Mundo” (24/10/00)
· Los internautas multiplican sus protestas contra la subida de tarifas. *Jaume Aràjol. “El País” (01-09-98)*
· Tarifa Plana: alt.best.of.internet.humor.spain. Alvy. “Microsiervos” (18-11-02)
· Campaña Tarifa Plana Ya!. Asociación de Internautas.

7.5. Hackmeeting

· Hackmeeting Italia
· Hackmeeting Península Ibérica
· Hackmeeting. Wikipedia.
· Barcelona acoge una reunión internacional de ‘hackers’. “El País” (22/10/00)

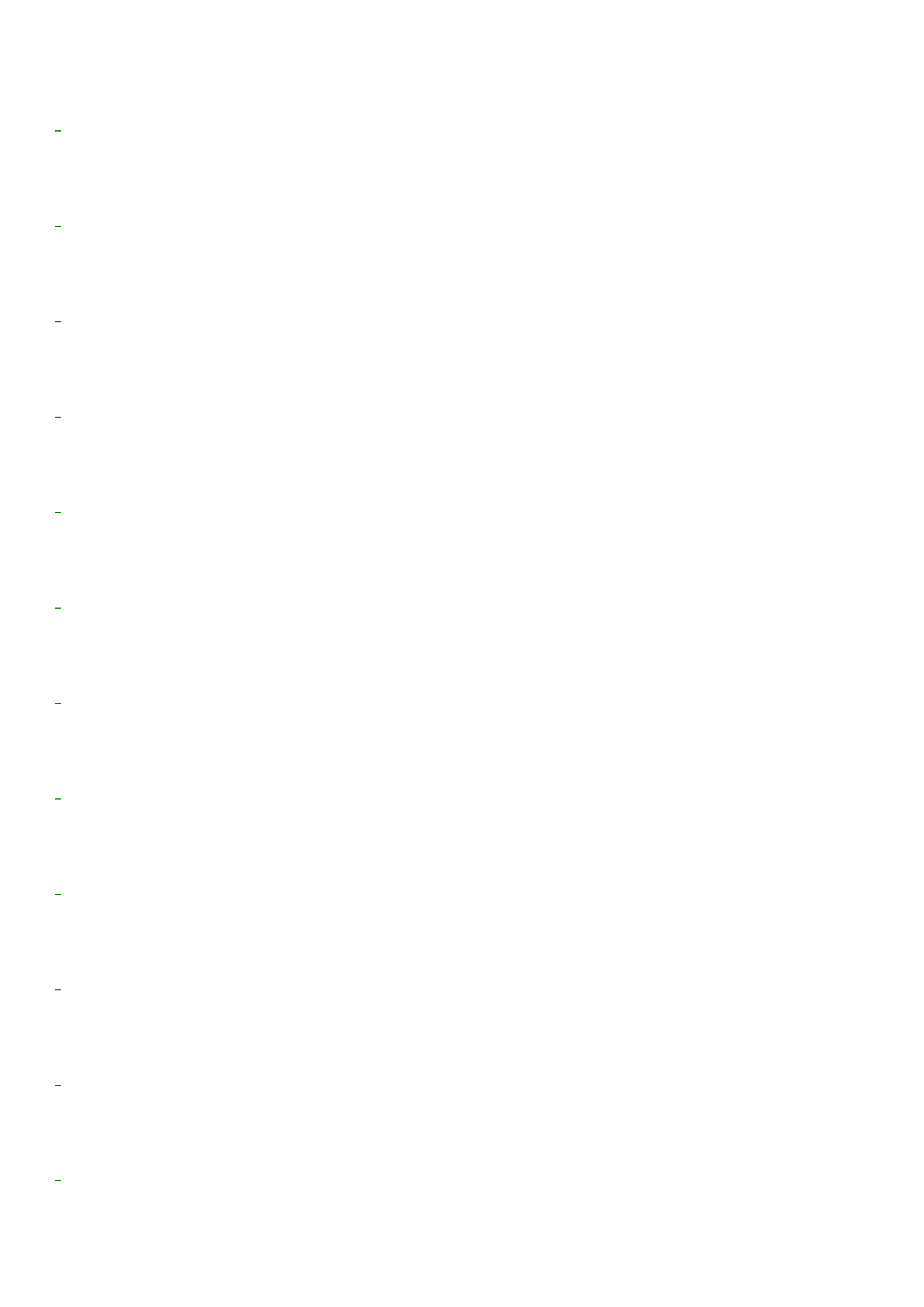
· De vuelta a las trincheras electrónicas. “El Mundo” (24/10/00)
· El Barcelona Hackmeeting a L’Internauta. “Vilaweb” (30/09/00)
· Hacklabs
· HackAndalus 1.0 Hackmeeting 5.0
· Charla del abogado David Bravo en el Hackmeeting de Sevilla
· Carta de David Bravo a la Sony. Lectura de la carta que David Bravo envió a los directivos de Sony durante el Hackmeeting Sevilla 2004.
· Hackelarre. Crónica del hackmeeting de Gernika. El weblog de izzack (17/11/07)
· Fotos Hackmeeting Madrid
· Labo 03. Escenario del MadHack02
· Centro Social El Laboratorio. Es.wikipedia.
· Trailer “Laboratorio 3, ocupando el vacío”. Documental de Kinowo Media. (27-08-07)
· Laboratorio 3, ocupando el vacío. Documental de Kinowo Media (2007)
· Flickr: The Hackmeeting Pool
· Fotos Hackmeeting Menorca
· Fotos Hackmeeting Menorca
· Fotos Hackmeeting Sevilla. Viernes
· Fotos Hackmeeting Sevilla. Sábado
· Fotos Hackmeeting Sevilla. Sábado noche
· Fotos Hackmeeting Sevilla. Domingo
· Fotos Hackmeeting Sevilla. Mix
· Introducción al hacktivismo. Txipi:blog (30/07/06)

7.5.1. CatHack

· Backup de las ezines CatHack
· Cathack en Zine Store
· CatHack!, hackers en catala

7.6. Los hacklabs

· Hacklabs.org
· Primera web del Hacklab Kernel Panic. Internet Archive (10-03-03)
· Primera web del Metabolik Hacklab. Internet Archive (06-06-02)
· Última captura de la Web del Downgrade Hacklab. Internet Archive (25-08-10)
· Hackespaces Spain
· Storia di FreakNet

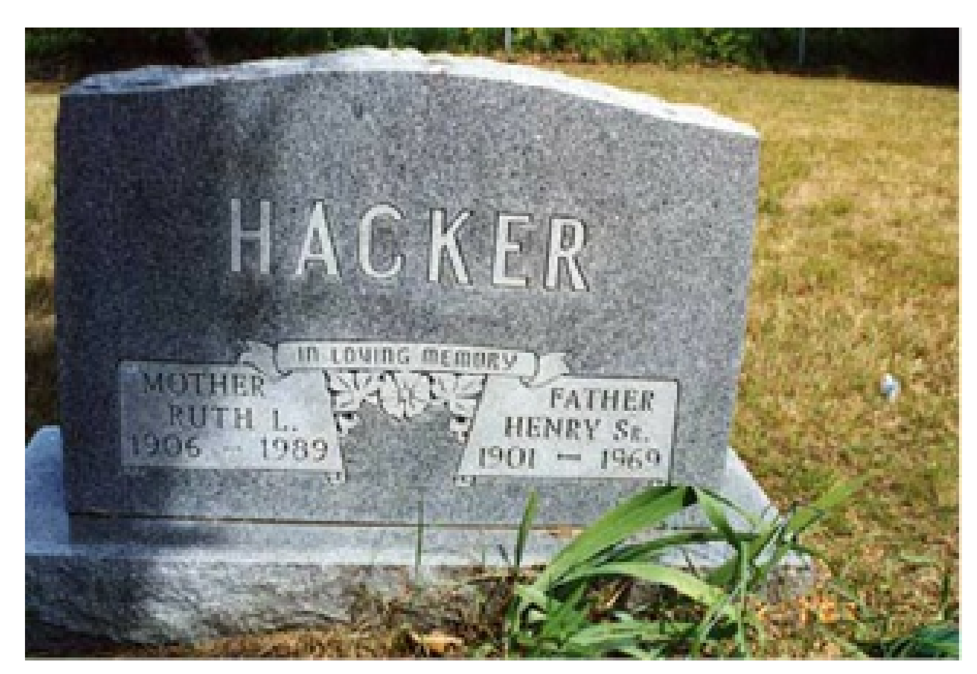


CAPÍTULO OCHO

El fin de la vieja escena

El fin de la vieja escena

Una noche oscura, que duraría casi una década, se cernía a principios del siglo XXI sobre el torrente de vitalidad que eran las *escenas* hacker. Llámalo hacerse mayor o el duro despertar en el Mundo Real, allí donde mandan las leyes de la naturaleza. Aquel viejo Sistema del que se reía el hacker que asaltaba sus redes, y el hacktivista que combatía sus ideas, seguía allí cuando se apagaba el ordenador, cínico e impertérrito.



Las trampas fueron el éxito y el dinero. En ellas cayeron los que iban más de listos, los que afirmaban tener la red en sus manos y no destruirla porque no les daba la gana. Los héroes de la entonces ya pomposa y muy egocéntrica escena hacker. No es extraño que quienes tenían el Poder en el Mundo Virtual viesen como un reto conseguirlo en el Mundo Real. El fallo fue no prever que ambos poderes son distintos, distintas sus reglas y sus contextos. Y tirarse de cabeza.

La seguridad informática se convirtió en negocio prácticamente de la noche a la mañana. Era el sueño siempre soñado, la vieja reivindicación, la razón, decían los hackers, por la que buscaban agujeros y los publicitaban: para que las empresas y otros organismos fuesen conscientes de la inseguridad de sus redes. Por fin, sus víctimas les hacían caso, invertían en seguridad y, ¡oh qué sueño maravilloso!, les pagaban por hacer lo que en los últimos años habían hecho a cambio de nada. Bueno, sí: de reconocimiento y aprendizaje.

Y no cobraban poco, no. Los precios de tonterías como pasar un escáner por una red se dispararon y con ellos los sueldos de aquellos chavales. Algunos crearon sus propias empresas de seguridad informática, pero el dinero estaba en las consultoras, que surgieron como setas. La primera, s21sec, contrató a buena parte de !Hispahack. O, según como se mire, finiquitó a !Hispahack. Los chavales, maravillados por aquel circo de dinero y reconocimiento (si te cogía una consultora significaba que eras bueno), firmaron contratos de confidencialidad que les prohibían lo que había sido la sangre y la esencia de la comunidad: compartir

información sobre sus investigaciones.

> El HACK hispano se murió en el momento que las empresas empezaron a capitalizar las ideas de los miembros de esta cultura… hasta ese momento todo era más sano… en el momento que empezaron a meter sus zarpas empresas para ganar dinero muchos de nosotros nos encerramos en una cúpula de cristal para que otros compañeros de profesión, que en otro tiempo fueron amigos de batallitas, no se enteraran de lo que estábamos trabajando y ganando dinero, porque pasaron de ser "Amigos" a "Competidores".**[1]**

Prácticamente no quedó hacker que tuviese tiempo para dedicar a sus amigos, ni conocimiento que transmitir fuera de los muros de su empresa. Los grupos morían por inactividad. La escena se fue al garete en cuatro días. O no exactamente: se transformó. De la comunidad hacker se pasó a la comunidad de seguridad informática. Y lo que antes eran rivalidades entre grupos se convirtieron en rivalidades entre consultoras, pues cada cual sentía los colores de la suya. Además, en muchas se contrataba a amigos de amigos, de forma que en una consultora acababan trabajando los del mismo grupo.

Ripe, en el penúltimo número de su 7a69ezine, a finales de 2002, firmaba con mano temblorosa la defunción de la "scene":

> ¿Panorama del under actual? Pues qué decir, de momento sigue bastante parado, al menos de cara al público. SET parece que se ha estabilizado (…). NetSearch sigue siendo una incógnita total, tras anunciar su retirada y su vuelta en alguna ocasión (…). En cuanto a Hispahack basta con decir que la web sigue prácticamente igual que cuando la inauguraron, con la diferencia de la actividad en los foros (que ha disminuido).**[2]**

La UnderCon, luz y guía de la vieja escena hacker, dejaría de celebrarse en 2004.

Hubo que pasar un tiempo hasta que esta situación cambiase y lo hizo cuando, después del estallido de la burbuja de las punto com, la onda expansiva llegó al negocio de la seguridad informática. Bajaron -o se racionalizaron- los sueldos y la vida haciendo *pentesting* se convirtió en -¡Oh Dios Mío!- rutina. Surgieron, como antaño en los grupos, los malos rollos y peleas de gallos entre los hackers de las consultoras. Ya no había colores que pudiesen maquillar aquel baño de realidad, de administrivia, de marketroides, de escribir tediosos informes, de decisiones empresariales ilógicas, del todo por la pasta. De aquello que, cuando eran salvajes, querían cambiar.

La escena hacker no fue la única en hundirse, sólo la más rápida. La comunidad del software libre sucumbió también, poco a poco. Los Grupos de Usuarios fueron siendo abandonados**[3]** porque se convirtieron en innecesarios. Habían servido para el primer embate, para popularizar el movimiento, pero la llegada de distribuciones como Ubuntu, que facilitaron muchísimo la vida a los novatos, hicieron inútil tal despliegue de ayuda.**[4]**

Por otra parte, el software libre no fue inmune al color del dinero. Al mismo tiempo que la administración pública se abría a proyectos libres, como la Junta de Extremadura con GNULinEX o Andalucía con GuadaLinex, cada vez más empresas entraban en el negocio. A partir de 1998 empezaron a desarrollar o apoyar

productos libres IBM, Oracle, Informix, SyBase, Corel, Silicon Graphics, Apple, Sun, Dell o Compaq[5]. En agosto de 1999, Red Hat salía a bolsa.[6]

Eran noticias vistas con orgullo y alegría por la comunidad libre, que las consideraba la prueba de que se avanzaba hacia la vieja broma de la comunidad linuxera: **“El plan para la dominación del mundo”**. Pero la euforia se apagó cuando se constató que algunas empresas compraban proyectos de software libre para dejarlos morir, como forma de aniquilar la competencia.

Este fue el caso, el más sangrante, de la compra de la empresa Sun por parte de Oracle, en 2009. Sun albergaba multitud de proyectos libres que no interesaban a Oracle[7], orientada a hacer dinero y punto. Así, MySQL, muy interesante para el negocio de bases de datos de Oracle, siguió con vida, mientras el sistema operativo OpenSolaris y la *suite* de ofimática OpenOffice eran dejados de lado.

> Aún así, si se abandona el soft libre es porque la comunidad no ayuda. En algunos casos no se permite la colaboración de la comunidad, en otros puede que la empresa aportara una parte muy grande. Por ejemplo en proyectos como Linux las empresas aportan la mayor parte del código.[8]



Hackmeetings y hacklabs también vivieron su decadencia, que culminaba en 2009 con la muerte, largamente anunciada, del Hacklab de Barcelona. El hacktivismo había asumido la reivindicación de lo que fue continuación natural del movimiento del software libre: la cultura libre y las licencias copyleft para los contenidos. El fenómeno explosionó en la primera década del siglo XXI, en el ámbito de la música, y siguió con menos empuje en la literatura pero triunfó en los blogs, el 99% bajo licencias Creative Commons.

Nuevos conceptos, inventos y personajes nacieron en la década que empezó con el temido efecto 2000; mientras la escena hacker, hasta el moño de trabajo, iniciaba su letargo. Los blogs fueron el *hit* de la década, pero hubo más: spam y más spam[9][10][11], la muerte de los grupos de noticias[12], el jaque mate a la SGAE[13], la escena P2P[14], 4chan[15], VirusTotal[16], *networking*, *honeypots*, estafas, cibercrimen, monitorización versus privacidad en las redes sociales[17], troyanos, wifi[18], escuelas de hackers[19], DVDJon[20], botnets[21], venta de fallos de seguridad[22][23], concursos internacionales de hacking[24] y, símbolo de la decadencia que vivía la comunidad a nivel planetario, la mala vida del phreaker más



famoso, el Capitán Crunch[25].

1. Boinas negras: Cuartango

No será hasta 2010 que el *hacking* se convierta en delito según el Código Penal del estado español. En reformas anteriores se ha ido preparando el terreno, como ilegalizar las herramientas de hacking, el conectarse a redes inalámbricas ajenas, usar tarjetas pirata de televisión digital o facilitar a terceros la forma de conseguir acceso no autorizado a un servicio, léase por ejemplo publicitar números 900.[26]

El hacking ya no es un juego impune y, para quien no quiera correr riesgos, proliferan los concursos de hacking[27] como forma de seguir ganando reputación y templar la adrenalida, pero en entornos seguros.

El primer concurso de este tipo en España se presentó en 2002, con el sugerente nombre de *Boinas negras* y organizado por el Instituto para la Seguridad en Internet. Los fundadores del Instituto eran viejos conocidos de la comunidad hacker: Juan Carlos García Cuartango, conocido internacionalmente por haber descubierto importantes agujeros de seguridad en productos Microsoft[28][29], y **Gonzalo Álvarez Marañón**, que desde 1997 editaba el boletín de seguridad informática Criptonomicón.



Cuartango, en 2010

El concurso *Boinas negras* fue muy bien recibido, con más de 4.000 inscritos en su primera edición[30], que ganó Alberto Moro, un santanderino de 26 años[31], más conocido como **Mandingo**. El segundo y último año, el ganador fue Pere Planiol, de 26 años[32][33]. Los premios del concurso eran tan originales como quesos, boinas, camisetas y un jamón.

2. Sombreros blancos: J.J.F. Hackers Team

El nombre *boinas negras* era un hack lingüístico: por una parte remitía de forma cómica y castiza al país donde se celebraba el concurso, por otro le daba un toque militar, de "boinas verdes", y por último era un guiño socarrón hacia la palabra de moda del momento: Hacker de sombrero blanco, también llamado *hacker ético*, contrapuesto al criminal informático o hacker de sombrero negro.

Ambos conceptos se los sacó de la manga la industria de la seguridad informática, deseosa de usar la palabra "hacker" en su publicidad pero temerosa de que, en vez de sugerir que un genial experto velaría por la seguridad de sus clientes, sugiriese la imagen de un criminal. El *hacker blanco* estaría pues al mismo nivel que *coca-cola sin cafeína* o *cerveza sin alcohol*, y significaría: *"Nuestros trabajadores son tan buenos técnicamente que pueden considerarse hackers, pero regidos por una ética que nunca pondrá a nuestros clientes en peligro, lo que nos legitima para cobrarle esas facturas tan altas"*.

> El hacker blanco es un experto en seguridad especialista en tests de penetración y otras metodologías para asegurar la seguridad de los sistemas de información de una organización. El término hacker ético lo acuñó IBM para sugerir un ámbito más amplio que sólo los tests de penetración.**[34]**

El grupo estadounidense L0pht fue el primero en llevar la bandera del *hacker blanco*, que la comunidad se tomó a broma. Pero L0pht no eran hackers de broma sino bastante buenos, autores del *crackeador* de contraseñas L0phtCrack. El grupo nació en 1992 y poco después creó la empresa L0pht Heavy Industries. En 1998 y ante el Congreso de Estados Unidos, que les invitó, aseguraron que era posible tumbar Internet en 30 minutos, lo que les hizo salir en todos los telediarios.



Desde España, los integrantes de J.J.F. / Hackers Team seguían con admiración los pasos de L0pht. En el sexto número de su ezine explicaban que habían asistido a una conferencia del grupo:

> Como anécdota decir que los de L0pth iban con sus camisetas oficiales y nosotros, ibamos con las nuestras también pero además con la gorras también, provocando que cuando entramos en la sala todo la gente se quedó boquiabiertos y los de L0pth se comenzaron al reir cuando vieron otro grupo Hacker entrar en la sala.**[35]**

JJF Hackers Team nació en 1996, de la mano de **Conde Vampiro** y **Mac Crack Bishop**.

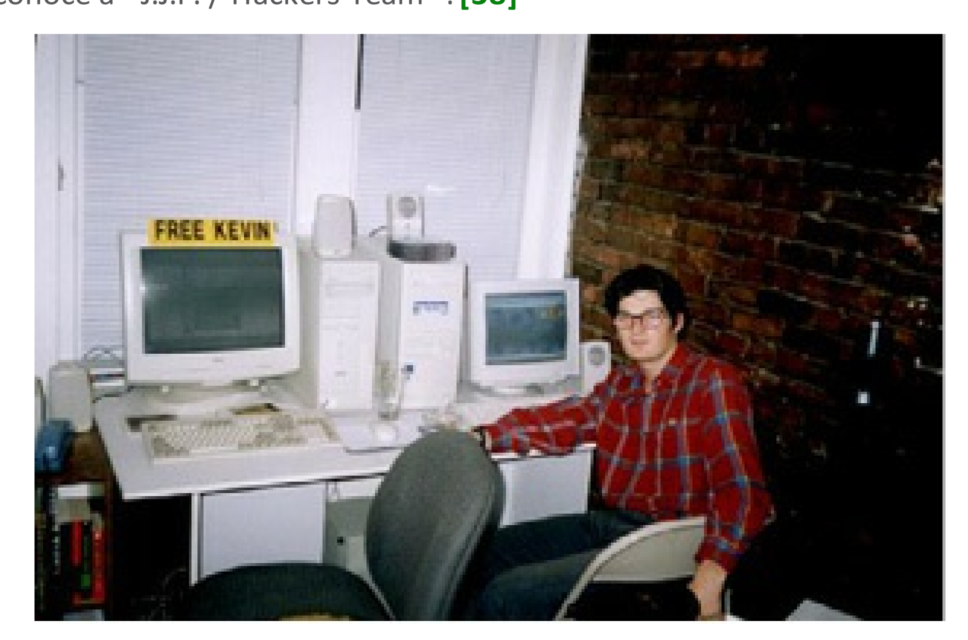
En 1998 entraron **Mr Elektro**, **Silent Motion**, **Jumpknown**, **Tasslehoff** y **Dr Binix**, cuyas edades oscilaban entre los 22 y 24 años. El último en unirse a ellos fue **Zhodiac**.



Integrantes de JJF Hackers Team. Foto sacada de su web

Durante tres años el grupo[36] desplegó una gran actividad, publicando programas y artículos sobre seguridad en multitud de sitios, incluída la reputada lista Bugtraq[37]. Pero la hazaña que más trascendió fue organizar la primera edición de la convención de seguridad informática No cON Name en Mallorca, de donde eran buena parte de sus integrantes. Por esta razón y también porque fueron los primeros en llamarse hackers blancos, JJF Hackers Team ha sido uno de los grupos más mediáticos de la escena.

> ¿Quien no conoce a - J.J.F. / Hackers Team -?[38]



Conde Vampiro, líder de JJF

El diario "El País" entrevistó a Conde Vampiro en 1999, quien explicaba qué era un hacker blanco:

> Son los chicos buenos, no tienen como meta penetrar sistemas ajenos, es la evolución de todo "hacker" que realmente quiera hacer algo útil con su experiencia. Hemos pensado que ir de piratas, como la mayoría, no conduce a nada y, además, debemos devolver el buen nombre que la palabra "hacker" representaba antes. Si alguien se ríe, pues cada uno a lo suyo, el tiempo dará la razón**[39]**

Y es que buena parte del "underground" se había tomado a risa lo del hacking blanco, como comentaba Hendrix, de SET, en otra entrevista con Conde Vampiro:

> -En el mundillo under ha habido un poco de cachondeo con el tema del "hackers blancos".
> -Esto lo unico que demuestra es desconocimiento.**[40]**



Logotipo del grupo tal como se conserva en su primera web, en Lycos

Cabría añadir que muchos de los que se reían se apuntaron después a la moda, queriendo o sin querer, ya que la empresa a la que fueron a trabajar usaba estos términos.

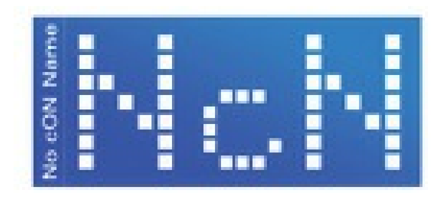
3. Materia gris: pr0j3ct m4yh3m

¿Y si no eras un hacker blanco ni negro, qué hacías? Pues eras un hacker gris y todo resuelto. ¡O amarillo![41]. También hubo quien se rió de tanto color: en 2002, el canal *#phrack* de la red EfNet creó el Pr0j3ct M4yh3m, con la intención de *provocar el holocausto whitehat*. El grupo español Digital Security Research (!dSR) se unió a ellos:

> Este proyecto tiene por misión ridiculizar a los whitehats, todos los que quieran ganar dinero con la industria de la seguridad y todo aquella que la rodea mediante la penetración de sus sistemas, ya sea a grandes compañías del sector, de personalidades con cierto nombre internacional o de grupos de hacking como en este caso.[42]

La mayor hazaña de !dSR[43] fue hackear los sistemas del respetado grupo alemán Chaos Computer Club (CCC) en 2004. Para ello usaron un fallo hasta entonces desconocido (*0day*) y consiguieron llegar hasta los datos privados de los participantes del *Chaos Computer Congress* de 2003, que hicieron públicos. La anécdota la proporcionó un miembro de CCC que descubrió el fallo que habían usado y se lo atribuyó. Entonces salió RomanSoft a explicar que lo había descubierto él y publicado en un reducido grupo.[44]

4. NoConName



Conde Vampiro y Zhodiac, de JJF Hackers Team, organizaron la primera edición del congreso de seguridad informática No cON Name (congreso sin nombre) o *NcN*[45], en 1999 en Palma de Mallorca.[46]

La *con* se celebraría anualmente en Palma hasta 2006 y después en Barcelona. Actualmente (2013) el equipo responsable son: **José Nicolás Castellano**, **Daniel Moll Cabrera**, **Àlex Quintieri**, **Àlex J. Clares**, **Pedro Valentino Sitaras**, **Daniel Agudo Garcia** y **Héctor Pantoja**

4.1. La profesionalización de los hackers

La No cON Name es un claro símbolo del cambio que vivía la comunidad hacker: aquellos hobbistas, muchos estudiantes, que se habían especializado en seguridad informática como si fuese un juego, con el nuevo siglo entran en el mundo laboral y trabajan en lo que había sido su afición, que se ha convertido en negocio.



Conde Vampiro y otro miembro de JJF Hackers Team

Empieza entonces la decadencia del “underground”, de las ezines. La que había sido *con* de referencia, la UnderCon, cae mientras la No cON Name emprende el vuelo. A pesar de haber nacido ambas de la escena hacker, las separa un abismo: la NcN muestra sin tapujos su orientación hacia la empresa y el nuevo concepto del *hacker blanco*, que ha dividido a la comunidad en buenos y malos aunque no ha inventado nada, pues antaño se dividió en *élite* y lamers, o *hacker* y cracker.

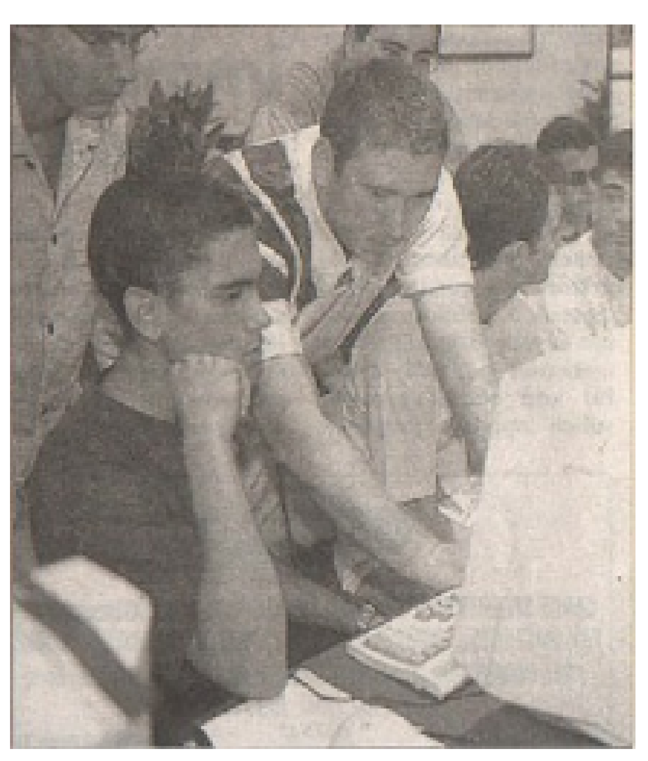
Por primera vez en un *con*, hay que pagar entrada (2.000 pesetas) y una consultora de seguridad informática de reciente creación, *Com & Media*, después S21sec, patrocina el evento. Esta consultora será la primera en España que usará el reclamo de los hackers blancos. Su fundador, el carismático **Miguel Fernández**, se atribuirá después ante los medios la idea de hacer el congreso, una trampa para cazar hackers:

> El camino que siguió éste empresario vasco para contratar a su equipo no fue fácil. (...) Miguel a sus 50 años decidió convertirse en hacker, se bautizó cómo Mikel y se lanzó a la red. Bajo ese nick fue entrando en contacto con algunos de los grupos de hacking españoles y empezó a conversar con ellos a través de chats. Realizados los primeros contactos y a través de la empresa Com&Media y la colaboración del grupo JJF Hackers Team, montó un encuentro de hackers, el primero de estas características en España.
>
> "La hicimos para ver exactamente que es lo que había en el mercado. Vino gente de toda España, gente que se conocía por sus nicks pero que jamás se habían visto personalmente. Estuvo bien pero sinceramente no había un gran nivel, los mejores, los realmente buenos no vinieron a una reunión que implicaba estar a cara descubierta. Era una cita demasiado abierta para que viniera la élite".**[47]**

Nico Castellano aclara por qué se trabajó con empresas y en clave blanca para tirar adelante la NcN:

> Lo bonito hubiese sido que nos cedieran unas instalaciones para 500 personas, y alguien nos regalara dinero para pagar los gastos, pero tuvimos que buscar un motivo y un apoyo para poder realizarlo. Tampoco fue un evento donde se contaba lo fácil que sería aplicar conocimientos de informática para hacer alguna pillería, sino que la temática de las ponencias era de investigación.**[48]**

4.2. La primera con



Yeyuno y uCaLu, en la No cON Name de 1999. La foto apareció en el periódico "Daily Bulletin" de 15 de diciembre de 1999, ilustrando una noticia que no tenía nada que ver, sobre la puesta en marcha del dominio *policia.es*

El congreso de 1999 se hizo del 23 al 25 de julio en un hotel de Palma de Mallorca[49][50]. Asistieron unas 50 personas, representantes de la escena hacker del momento: grupos como Undersec, HackUMA, !Hispahack, SET y los mallorquines OiOiO's Band, que co-organizaban la *con*.

También asistieron emprendedores que estaban creando las primeras consultoras especializadas en seguridad informática, como Alfonso Lázaro Téllez, de *IP6 Seguridad*[51], y Mikel Fernández, fundador de *Com & Media*. El abogado Carlos Sánchez Almeida[52] y el profesor de la universidad de Deusto Jorge Garcés dieron sendas charlas. Incluso andó por allí un equipo de periodistas del programa *Documentos TV* de Radio Televisión Española, que realizaba un reportaje sobre la comunidad hacker.[53]

Al final, Com & Media contrató a algunos asistentes[54], que serían la semilla del equipo de hackers éticos de la empresa. Entre ellos estaba Zhodiac:

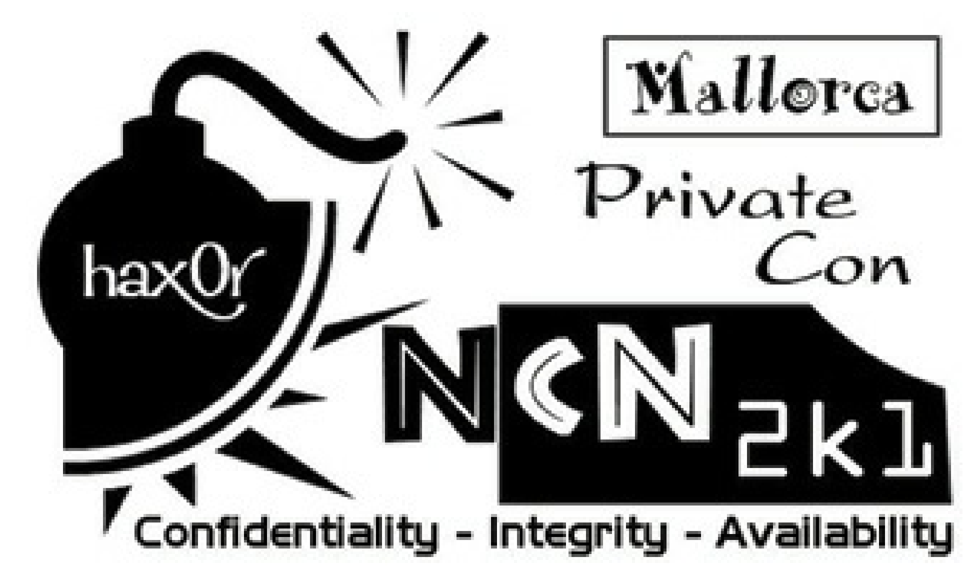
> Los técnicos iniciales fuimos: Alfonso Lázaro (no afiliado a ningún grupo pero presente en la NcN), LLuís Mora (jfs) y Netsavage de !Hispahack, dos locales de la Universidad de San Sebastián y yo. Luego (en algunos casos anyos o meses mas tarde) se fichó a más gente de !H como DrLethan, Slayer, Necronoid y más tarde gente de otros grupos como CPNE, Vieja Guardia (Darkcode)... rwxrwxrwx (conocido como 7) y bastante más tarde gente como Griyo.[55]



MeTalSluG diseñó los banners de la NoConName

La nota negativa fueron las tiranteces entre los organizadores, que llevaron a la disolución del grupo el mismo día que acabó la No cON Name, lo que hizo pensar que el congreso había muerto, pero no: reapareció en 2001 como una reunión privada impulsada por Conde Vampiro y Nico Castellano:

> Yo nunca formé parte de JJF, aunque conocía a casi todos. Conde Vampiro venía a la isla en vacaciones y quedábamos de vez en cuando. Llegamos a apodarnos el "*p0mada hax0r team*". Hablando con Conde salió la posibilidad de hacer otra CON pero dijo que debía ser algo privado y que debíamos moverla con cautela.[56]

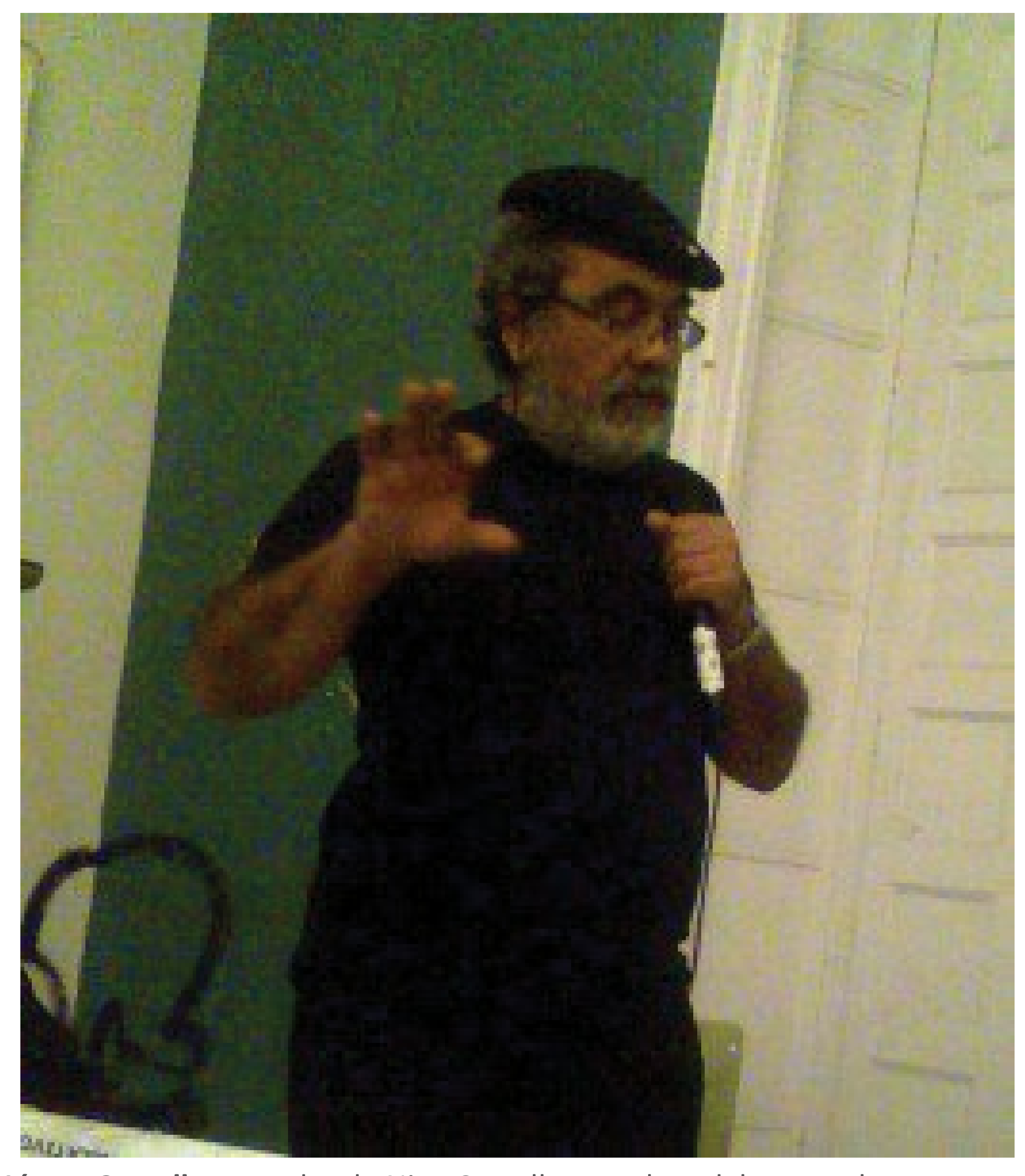


El año anterior la Guardia Civil había detenido a medio “underground” en la Operación Millenium y todos tenían aún el miedo en el cuerpo, razón por la que esta edición no fue pública.[57]

4.3. NcN 2k2: Ahora en serio

El buen sabor de boca del encuentro privado animó al grupo a seguir adelante y buscar nuevos patrocinadores pero, como explica Nico Castellano, *“¿qué empresario en España iba a poner dinero en una reunión que organizaban 7 chavales de 20 años?”*[58].

Conde Vampiro, **DS**, **MKiller**, **NAISMITH**, **MeTalSluG**, **WaRMaKeR** y **Yeyuno** (Nico Castellano) empezaron a buscar, pero su edad se convirtió en un problema para encontrar no sólo financiación sino incluso un sitio donde celebrar el congreso:



Hugo Héctor Castellano, padre de Nico Castellano y alma del evento hasta su muerte, en 2012[59][60]

> Nico contactó con algún Banco donde nos iban a prestar las instalaciones del Pueblo Español y al presentarse en la cita y encontrarse con un chaval de 18 años trajeado, no le hicieron demasiado caso y de préstamo pasó a ser alquiler a 1 millón de pesetas. Era primeros de mayo del 2002, a mes y medio del evento, y no teniamos lugar donde realizarlo, estabamos bastante desanimados, y el GRAN HUGO agarró a Nico y le dijo que aunque vinieran 3 personas y hubiera que hacerlo en el salón de casa, que la NcN se haría sí o sí.[61]

Nico pidió entonces ayuda a la asociación *Balearikus Party*, que organizaba una exitosa LAN-party en Mallorca. Su intercesión fue vital: **Modesto Agudo** y **Gabriel Ginard** consiguieron, en sólo un mes, un patrocinio de 1.200 euros de la Fundació Ibit y que el Govern Balear cediese la sala de actos del parque tecnológico ParcBit a la *con*.

En su primera época, de 2002 a 2006, dieron conferencias en la No coN Name destacados nombres de la comunidad que ahora se llamaba *de seguridad informática*. Otro cambio respecto a la UnderCon era que los ponentes ya no se presentaban con un *nick* y el nombre de su grupo de hackers, sino con su nombre completo y la empresa para la que trabajaban: s21sec, SIA, Auditoría Informática Balear, @Stake, InetSecur, ImmunitySec, Internet Security Auditors. Esta última ha

sido la más fiel al congreso, que esponsoriza desde 2004.

Destacan entre las decenas de ponentes de la NcN Gema Gómez, Albert Puigsech, Javier Olascoaga, Vins Vilaplana, Daniel Cabezas, Nicolás Waisman, Andrés y Miguel Tarascó, Ramón Pinuaga, Alejandro Ramos, David Barroso, Christian Martorella, Ero Carrera, Raoul Chiesa y César Cerrudo.

En 2007 cambió el gobierno de las Illes y la *con* se quedó sin subvención[62]. Reapareció en 2010, en Barcelona.



Ganadores del concurso de Internet Security Auditors en NcN 2006: Pedro Andújar, Andrés Tarascó Acuña y Javi 'Ds' Olascoaga. Entrega el premio Daniel Fernández Bleda



Asistentes a la NcN 2006, con camisetas de S21sec

5. El lado oscuro

Y así fue como buena parte de la comunidad se pasó al bando de los *blancos*, aparcó sus *nicks* y empezó a trabajar con la antes temida policía. Pero el lado oscuro es fértil y no sólo no notó el vacío sino que se llenó aún más. Esta vez no con chavales que rompían límites para aprender pero tenían una ética, sino con chavales dispuestos a llenarse rápidamente los bolsillos con el cibercrimen. Y así fue como ambos bandos vivieron un espectacular crecimiento de sus respectivos negocios: el de la seguridad informática y el de las mafias de la red.

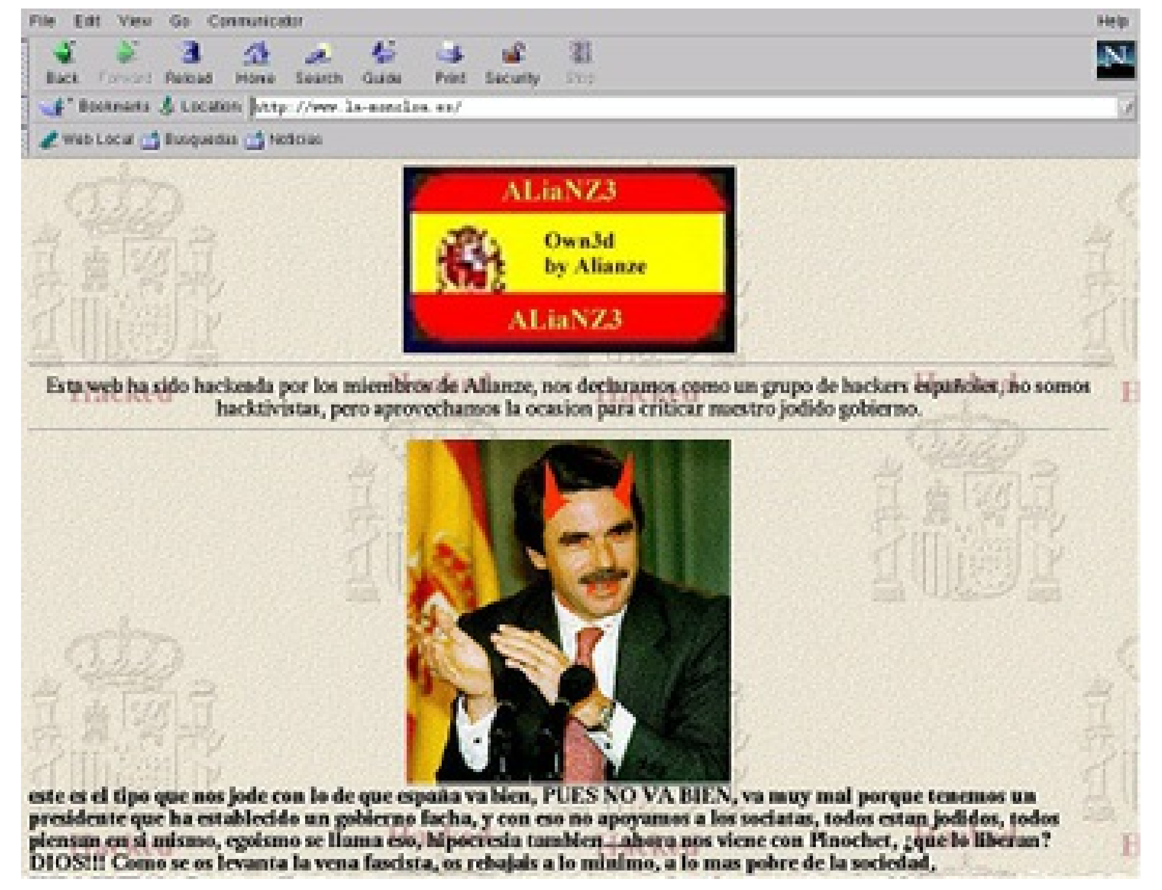
España llegó a ser en 2007 uno de los países con más ordenadores infectados del mundo**[63]**, pero era sólo una víctima, el grueso de los malos estaba en los antiguos países del este europeo, Brasil y América Latina.

Hubo quien se quedó en el lado oscuro no por interés crematístico sino por neurosis diversas, como el afán de reconocimiento o la pura destrucción. Sus armas serán las mismas del cibercrimen, por ejemplo las botnets de miles de ordenadores que bombardean redes. Es una nueva generación de hackers, los script kiddies, para quienes es más importante que se vean sus acciones que la calidad del hack que hay detrás.

Por eso a los *script-kiddies* les gustan los *defaces*, que son pura imagen. Mejor los *massdefacements*: modificar de una sola tacada cientos o miles de páginas web. Esto se consigue entrando en proveedores de alojamiento que tengan muchos clientes, de forma que el asalto cunde mucho más, pues por el trabajo de entrar en un sitio se consigue la visibilidad de modificar cientos o miles de webs.

Los *kiddies* pusieron también de moda los ataques distribuidos de denegación de servicio (DDoS), que consistían en bombardear un sitio desde miles o decenas de miles de ordenadores, de forma que fuese muy difícil defenderse contra todos a la vez. El primer DDoS que impactó al mundo dejó KO a los grandes de Internet en el 2000: Yahoo!, ZDNet, CNN, E-Bay, E*Trade y Amazon. A este lo siguieron DDoS por todo tipo de motivos, desde chantajear a empresas hasta vengarse de alguien que ha insultado al *kiddie* en un foro.

España no es ajena al nuevo panorama y la violencia también se adueña de lo que había sido la escena hacker. ¿Por qué esperar años aprendiendo y hackeando hasta ganarse el respeto de la comunidad (¿qué comunidad, por cierto?), si haciendo el gamberro sales en la tele?. Eso debió pensar **Jocanor** quien en 2004, con su grupo Unixcrew, se dedicaba a asaltar los sistemas de medios de comunicación, como la COPE, Telemadrid, Popular Televisión. Quizás pensando que así se haría famoso más rápido.



Otro grupo que destacó fue Alianz3, cuyo líder se dice que era hijo del director de un importante periódico español[64]. La gran hazaña de Alianz3 fue el *deface* de la web de La Moncloa, en 1999, para poner una foto del entonces presidente del gobierno español, José María Aznar, con cuernos y colmillos.[65]

6. Los últimos del "underground"... y la nueva escena

Ante este panorama, los veteranos que querían seguir en el lado oscuro (aunque de día trabajasen en consultoras) eran cada vez menos. Un repaso de los grupos que asisten a las dos últimas ediciones de la UnderCon da una idea de quién quedaba en el "underground": Fuego Fatuo, IaM y Dark Raver de The Old School, GriYo de 29A, Pope de Undersec, The Den of the Demons, Pancake de CatHack y Warezzman de CPNE.

Otra dato que certifica el parón de la escena es que los pocos grupos que se crean a partir del 2000 no tienen sangre nueva: sus miembros son refugiados, damnificados de la decadencia de otros grupos, que a veces siguen éxodos saltando de un sitio a otro, como el que llevó a parte de La Vieja Guardia a formar Total Coredump y, de aquí, Kernelpanik. O The Old School, que recogía a supervivientes de los naufragios de !Hispahack y CPNE.

Como explicaba en 2007 uno de los últimos hackers auténticos, el inglés Adam Laurie, lo que quedaba de la comunidad en Europa y Estados Unidos no tuvo otro remedio que esconderse.

> El hecho de que la investigación legítima sea accesible a los chicos malos, sumado a las nuevas leyes, ha provocado que la comunidad se haga más "underground". Esto nos hace más difícil operar y existir como comunidad, porque la gente tiene miedo de exponerse demasiado y ser detenidos porque publicaron algo, o que esto sea utilizado por alguien con fines criminales.**[66]**



Pero esta travesía en el desierto tiene un feliz final y es la resurrección de la comunidad y una nueva escena hacker, impulsada por las jóvenes promesas que ya se intuían al final del ciclo anterior, más algunos veteranos aún con ganas de "jugar". No son muchos pero sus nombres y apodos están tras las diferentes iniciativas que llevarán al resurgimiento. Uno de los primeros signos de vida de esta

nueva escena son los hackers españoles que, a falta de ezines en su idioma, ya todas muertas, publican en la veterana revista electrónica Phrack[67]: **Zhodiac** en 2001[68], **Pluf** y **Ripe** en 2005[69], **Ilo** también en 2005[70], **Dreg** y **Shearer** en 2008[71], **Pancake** en 2009[72] y **Blackngel** en 2009[73] y 2010[74]

En 2007 y relacionado estrechamente con el colectivo 48bits, formado por algunos de los ya citados más nombres emergentes como **Rubén Santamarta (madalenas)**, **Mario Ballano (Nullsub)** y otros, aparece ¡por fin! un nuevo grupo de hackers en el estado español. Se llaman **Pandas with Gambas** y se dedican a participar en concursos de hacking, como el reputado "Capture The Flag" de la convención norteamericana DefCon. Entre sus integrantes hay gente más que destacada, como **Sha0** y Pancake, pero se niegan a revelar sus identidades a la prensa[75]. En 2009 el grupo cambia de nombre, se llamará **Int3pids**. Shao y Pancake lo dejan, mientras siguen **RomanSoft**, **Whats**, **Dreyer**...



En 2008, *48bits* pone en marcha una nueva *con* dirigida al "underground": la **LaCon**[76][77][78]. Como antes la UnderCon, la Lacon se concibe como una reunión de amigos, la admisión está reservada a gente con altos conocimientos y se accede por invitación. La empresa de seguridad informática Hispasec la patrocina en sus dos primeras ediciones, cuando se celebra en Málaga y reúne a un par de decenas de personas. Posteriormente se decide hacerla cada año en un sitio diferente y organizada por gente diferente.

Son las semillas que necesitaba la escena para resurgir. Un año después, cuatro veteranos hackers, **Román Medina-Heigl** (RomanSoft), **Román Ramírez** (Patowc), **Javier Olascoaga** y **Raúl Jover** deciden poner en marcha un congreso anual de seguridad informática abierto al público en general. Se hará en Madrid, se llamará Rooted CON y verá la luz en 2010.[79]

La Rooted tendrá la suficiente sabiduría para no quedarse en un congreso de empresas y corbatas y hacer guiños a todo lo que queda en pie, desde los CERTs o la Guardia Civil hasta los "hardware hackers" y expertos en ingeniería social. La

RootedCon habla en el lenguaje de la comunidad y por eso Rampa y Savage cuentan batallitas en la primera edición, mientras nuevas glorias como Chema Alonso, Sebastián Guerrero, Nighterman, Reversemode escuchan con atención.

El “under” llena las butacas o se sienta en el suelo con el móvil en la mano. Reviven los hackers, los viejos con sus viejos nicks o con uno nuevo o con nombres reales que nada quieren que se sepa del pasado, y los nuevos que han crecido en esta década de crisis, de aislamiento.



Una lista de correo[80] es la guinda perfecta para crear -o recrear- de nuevo la comunidad, con sus héroes y antihéroes y, como no, una revista lo contará: Security By Default. Porque las redes están hechas de material inerte, pero quienes viven en ellas son humanos, inexorablemente obligados a seguir ciclos de esplendor y muerte. Y esplendor de nuevo. Esta vez (2013) de la mano de la *escena hacker de Madrid*, como antaño fueron la *escena murciana* y la catalana y mucho tiempo atrás, la *escena de Zaragoza*.

7. Notas

1. ↑ uCaLu, de Undersec, en conversación privada
2. ↑ 7a69 14 (21/10/02)
3. ↑ Grupos de usuarios. Linux-es
4. ↑ El secreto de Ubuntu. Mercè Molist para “Ciberpaís” (16-03-09)
5. ↑ La imparable historia del software y la cultura libres. Mercè Molist para “Ciberpaís” (11-02-08)
6. ↑ La entrada en bolsa de Red Hat marca el asalto del software libre a la empresa. Mercè Molist para “Ciberpaís” (08-99)
7. ↑ A Year After: The Open Source Projects. Castellers v2 (16-01-11)
8. ↑ Xavier Barnada. Twitter (06-08-13)
9. ↑ El correo basura crece exponencialmente, dos años después de su prohibición. Mercè Molist para “Ciberpaís” (01-07-04)
10. ↑ España es el quinto emisor de correo basura del mundo. Mercè Molist para “Ciberpaís” (16-11-06)
11. ↑ Los proveedores españoles de Internet se unen para combatir el correo electrónico fraudulento. Mercè Molist para “Ciberpaís” (23-03-07)
12. ↑ Los grupos de noticias se mueren. Mercè Molist para “Ciberpaís” (17-06-09)
13. ↑ La mujer que desafió a la SGAE. Mercè Molist para “@rroba” (03-09-07)
14. ↑ Entrevista Jaj: Animersion Team. Mercè Molist para “@rroba” (22-09-08)
15. ↑ 4chan, los bastardos de la red. Mercè Molist para “Ciberpaís” (03-09-09)
16. ↑ El servicio español de seguridad más internacional nació en Málaga y se llama VirusTotal. Mercè Molist para “Ciberpaís” (06-11-08)
17. ↑ ¿Redes sociales o monstruos comedatos?. Mercè Molist para “Ciberpaís” (08-10-08)
18. ↑ La mayor red inalámbrica del mundo está en Catalunya. Mercè Molist para “Ciberpaís” (28-08-06)
19. ↑ Escuela de hackers para adolescentes. Mercè Molist para “Ciberpaís” (25-03-03)
20. ↑ La industria del DVD se da de bruces con Internet. Mercè Molist para “Ciberpaís” (03-02-00)
21. ↑ José Nazario: “Con una botnet se pueden ganar miles de dólares al día”. Mercè Molist para “Ciberpaís” (25-06-07)
22. ↑ Rubén Santamarta: “Las mafias me han ofrecido cheques en blanco”. Mercè Molist para “Ciberpaís” (23-01-08)
23. ↑ Los descubridores de fallos informáticos cotizan al alza. Mercè Molist para “Ciberpaís” (12-02-10)
24. ↑ Un grupo español logra el primer puesto en las semifinales del concurso de hacking más legendario. Mercè Molist para “Ciberpaís” (11-07-08)
25. ↑ El ocaso del “phreaker“ más famoso de la historia. Mercè Molist para “Ciberpaís” (25-01-07)
26. ↑ El nuevo Código Penal crea incertidumbre en la red. Mercè Molist para “Ciberpaís” (21-09-04)
27. ↑ Recopilatorio de soluciones a retos en español. Vicente Motos. Hack Players (01-10-10)
28. ↑ Microsoft es noticia. Jesús Cea. “Linux Actual” (14/12/98)
29. ↑ Los retoños de Cuartango. *Boletín del Criptonomicón (19/11/98)*
30. ↑ La comunidad hacker busca a sus ‘boinas negras’. Olalla Cernuda. “El Mundo” (14-05-02)
31. ↑ Más de 4.000 inscritos en un original concurso de “hacking”. Mercè Molist para “Ciberpaís” (09-05-02)
32. ↑ Casi 3.000 participantes al asalto de una web de concurso. Mercè Molist para “Ciberpaís” (25-06-03)
33. ↑ El regreso de los Boinas Negras
34. ↑ White hat hacker. En.Wikipedia
35. ↑ - J.J.F. / HACKERS TEAM - ESTUVO CON L0PHT EN MIT. Noticias underground. -J.J.F Hackers Team Journal 06 (1998)
36. ↑ jjf.org. Web oficial de JJF Hackers Team
37. ↑ Zhodiac. J.J.F. / Hackers Team warns for SSHD 2.x brute force password. Bugtraq (13/05/99)

38. ↑ Charlando con J.J.F. / Hackers Team. 7a69ezine 08 (3-12-00)
39. ↑ Hackers blancos a la española. Mercè Molist. “Ciberpaís” (1999) *(no se conserva copia del artículo aparecido en el diario)*
40. ↑ En línea con... Conde Vampiro. Hendrix. SET 20 (18-08-99)
41. ↑ Beyond black, white, and grey: the Yellow Hat Hacker. ratel. Full Disclosure mailing list (18-11-02)
42. ↑ Hackeos memorables: Chaos Computer Club. Security By Default (16/06/09)
43. ↑ Index of /stuff. Digital Security Research]
44. ↑ Hackeos memorables: Chaos Computer Club. Security By Default (16/06/09)
45. ↑ Web oficial No cON Name
46. ↑ Current members. JJF Hackers Team Journal 08 (30-11-99)
47. ↑ Hackers, los intrusos en la red (Que es un hacker). Laura Cortada. “Públic” (06-00)
48. ↑ Nico Castellano, en conversación privada
49. ↑ NcN-info. JJF Hackers Team
50. ↑ El “under” hispano se hace fuerte en Mallorca. Mercè Molist (07/99)
51. ↑ Triunfo de 4 “hackers éticos” españoles. Xombra (06-02-05)
52. ↑ El Hacking ante el Derecho Penal: Una visión libertaria. Carlos Sánchez Almeida. Ponencia presentada en la NcN 1999 (23/07/99)
53. ↑ Internet Zona Peligrosa. Documentos TV. La 2. Radio Televisión Española
54. ↑ Hackers al rescate. Mercè Molist (31-05-00)
55. ↑ Zhodiac, en conversación privada
56. ↑ Nico Castellano, en conversación privada
57. ↑ Naismith, en conversación privada
58. ↑ Nico Castellano, en conversación privada
59. ↑ En memoria del “comandante” Hugo Castellano. Chema Alonso. Un informático en el lado del mal (03-12)
60. ↑ Mensaje de Hugo Castellano en RootedCON 2012. José Nicolas Castellano. Vimeo (04-03-12)
61. ↑ Naismith, en conversación privada
62. ↑ Entrevista a Nico Castellano de NoConName. *Chema Alonso. Un informático en el lado del mal (25-08-11)*
63. ↑ Los ordenadores “zombi” invaden España. Mercè Molist para “Ciberpaís” (15-01-07)
64. ↑ Televisión Española aborda el tema de los “hackers”. Antonio Ropero. Una-al-día (14-01-00)
65. ↑ Asalto a la Moncloa. Ildefonso Olmedo. “Diario del navegante”. “El Mundo” (15-08-99)
66. ↑ Adam Laurie: “La mejor forma de entender algo es romperlo”. Mercè Molist para “@rroba” (19-07-07)
67. ↑ Españoles por la Phrack. David Barroso. Lostinsecurity (30-03-13)
68. ↑ HP-UX (PA-RISC 1.1) Overflows. Zhodiac. “Phrack” #58 (28-12-01)
69. ↑ Advanced antiforensics : SELF. ripe & pluf. “Phrack” #63 (01-08-05)]
70. ↑ Process Dump and Binary Reconstruction. Ilo. “Phrack” #63 (01-08-05)]
71. ↑ Phook - The PEB Hooker. Shearer and Dreg. “Phrack” #65 (11-04-08)
72. ↑ Binary Mangling with Radare. Pancake. “Phrack” #66 (11-06-09)
73. ↑ Malloc Des-Maleficarum. blackngel. “Phrack” #66 (11-06-09)
74. ↑ The House Of Lore: Reloaded ptmalloc v2 & v3: Analysis & Corruption. blackngel. “Phrack” #67 (17-11-10)
75. ↑ Un grupo español logra el primer puesto en las semifinales del concurso de hacking más legendario. Mercè Molist para “Ciberpaís” (11-07-08)
76. ↑ LaCon 2009, ¿pública o privada?. Víctor Manuel Álvarez y Bernardo Quintero. Blog del Laboratorio Hispasec (29-10-08)
77. ↑ Con la resaca de LaCon. Victor Manuel Alvarez. 48bits (21-09-08)
78. ↑ Grupo LaCon en Linkedin
79. ↑ La Historia de la RootedCON. RomanSoft (03-05-10)
80. ↑ Contacta. Rooted CON

8. Enlaces externos

· Lacon 2k13-

8.1. Juan Carlos García Cuartango

· Cuartango: “Los agujeros vienen a mi”. *Algunos hackers buenos*. Mercè Molist (05/07/01).
· Juan Carlos García Cuartango: la pesadilla de Microsoft. Olalla Cernuda. “El Mundo” (03/08/99).
· Encuentro digital con Juan Carlos Garcia Cuartango. Elmundo.es (23/04/01).
· Medidas provisionales e imprescindibles a adoptar de inmediato. Juan Carlos García Cuartango. Kriptópolis (03/04/01).
· Entrevista digital con Juan Carlos García Cuartango. Elpais.com (02/11/05).
· Nuevo agujero descubierto por Cuartango. Boletín del Criptonomicón (24/02/99).
· Comparecencia de Juan Carlos García Cuartango en el Senado. (27/03/01).
· Cuartango demuestra que Microsoft puede instalar programas sin avisar. Hispasec (22/02/00)
· El ingeniero que obligó a replantear el ‘Explorer’. Carmen Jané. “El Periódico” (02-09-12)
· iZhal: una comunidad dedicada al hacking. RS-Labs (19-10-02)

8.2. J.J.F. Hackers Team

· Todo sobre la tecnología Tempest. Antigua web del grupo (27-10-97)
· Cool Crackz. Antigua web del grupo (1997)
· Virus. Antigua web del grupo (1997)
· JJF Hackers Team. Antigua web del grupo (1997)
· Bienvenidos a Crackilandia. Antigua web del grupo (1997)
· Hack una web. Antigua web del grupo (30-12-96)
· La Guia Universal del Hacker en el IRC v. 1.0. JJF Hackers Team.
· Hackers, los intrusos en la red (Que es un hacker). Laura Cortada. Revista Públic (06-00)
· Primer número de JJF Hackers Team. Proyectos, peticiones, avisos. SET Staff. SET 13 (13-02-98).
· - J.J.F. / Hackers Team warns for SSHD 2.x brute force password. Bugtraq (13/05/99)
· Files from J.J.F. / Hackers Team. Packetstorm Security (17-08-99)
· Ataque por fuerza bruta a sshd2 v.2.0.11. Foro Hackhispano (12/01)
· Deteccion de Intrusos en un sistema unix. Conde Vampiro. - J.J.F. / Hackers Team - Security Documentation (1998)
· Como implementar SSL para servidores Apache. Dr Binix. - J.J.F. / Hackers Team - Security Documentation (1999)
· Web Spoofing 1.0. Dr Binix. - J.J.F. / Hackers Team - Security Documentation (1999)
· La Verdad Y La Mentira en el Mundo Del Hacker. Conde Vampiro. Raregazz 09 (10-10-97)
· El “under” hispano se hace fuerte en Mallorca. Mercè Molist. “Ciberpaís” (07/99)
· Charlando con - J.J.F. / Hackers Team -. Ripe. 7a69 08 (12-03-00)
· NcN. El congreso de Palma. Ripe. 7a69 14 (19-09-02)

8.3. Digital Security Research

· Digital Security Research
· Despedida a CRG en Madrid
· #phrack
· THE PROJEKT MAYHEM TOOLKIT

· Project Mayhem 2012

8.4. NoConName

· No cON Name web oficial
· Grupo Noconname en Facebook
· No cON Name en Twitter
· Asociación No cON Name en Linkedin
· Diario de la NcN´99. Tasslehoff. JJF Hackers Team.
· La columna de opinión: Noconname 2005*. Carlos Mesa. Informativos.ws #73 (25-09-05)*
· "Podemos robar una base de datos en 5 segundos". Mercè Molist para Ciberpaís "El País" (03-10-06)
· "Podemos robar una base de datos en 5 segundos". Mercè Molist. VSantivirus (17-10-06)
· NoConName – Attack Surface Analysis of Windows CE/Mobile 5. Ollie Whitehouse. Symantec Oficial Blog (29-06-09)
· Vuelve la NoCONname en Barcelona. Laboratorio Hispasec. Una-al-día (30-09-10).
· Nos vamos a la Noconname!!. Pedro Sánchez Cordero. ConexionInversa (11-10-10).
· Resumen de NoConName 2011 #ncn2k11. Lorenzo Martínez. Security By Default (19-09-11)
· "Las empresas no se toman la seguridad en serio". Mercè Molist. Ciberpaís - El País (07-10-11)
· Crónica NoConName 2012 - Día 1 #ncn2k12. Lorenzo Martínez. Security By Default (03-11-12)
· NoConName 2K12. Longinos Recuero Bustos. Los mundos de L0ngin0x (05-11-12)
· Malware intelligence ppt-slides. Sebastián Guerrero en NcN 2011 (17-09-11)
· Vídeos de las conferencias de la BkP 2001. René Mérou. Weblog BULMA 825-11-02)
· La fal.lera webloguera. Mercè Molist para "Avui" (28-05-03)
· Canción del Software Libre. José Luis Maquieira. Himno de Badopi.

Hackstory.es Autora

Mercè Molist Ferrer. Periodista especializada en Internet desde 1996. He escrito en múltiples medios, entre ellos los periódicos El Mundo, El País, La Vanguardia y revistas *Web* y *@rroba*. En *El País*, donde trabajé más de 10 años, me encargaba de investigar en exclusiva todo lo relacionado con seguridad informática y comunidades hacker, así acumulé mucha documentación y contactos que he volcado en el proyecto Hackstory y en este libro.

Hackstory.es Advertencia

Algunos enlaces pueden no funcionar.

Hemos puesto especial atención en asegurar que los enlaces externos a este libro estén activos. Pero por la naturaleza cambiante de la red, así como por la especial naturaleza de este trabajo de investigación, que toca acontecimientos muy lejanos en tiempo red, los enlaces que aparecen en Hackstory.es son vulnerables a la desaparición o, con suerte, sólo cambio de sitio. Es por ello que no podemos asegurar que todos los enlaces funcionen correctamente.

Aprovechamos para agradecer la ingente tarea del proyecto Internet Archive que nos ha permitido recuperar buena parte de los contenidos de este libro, que de otra forma se habrían perdido.